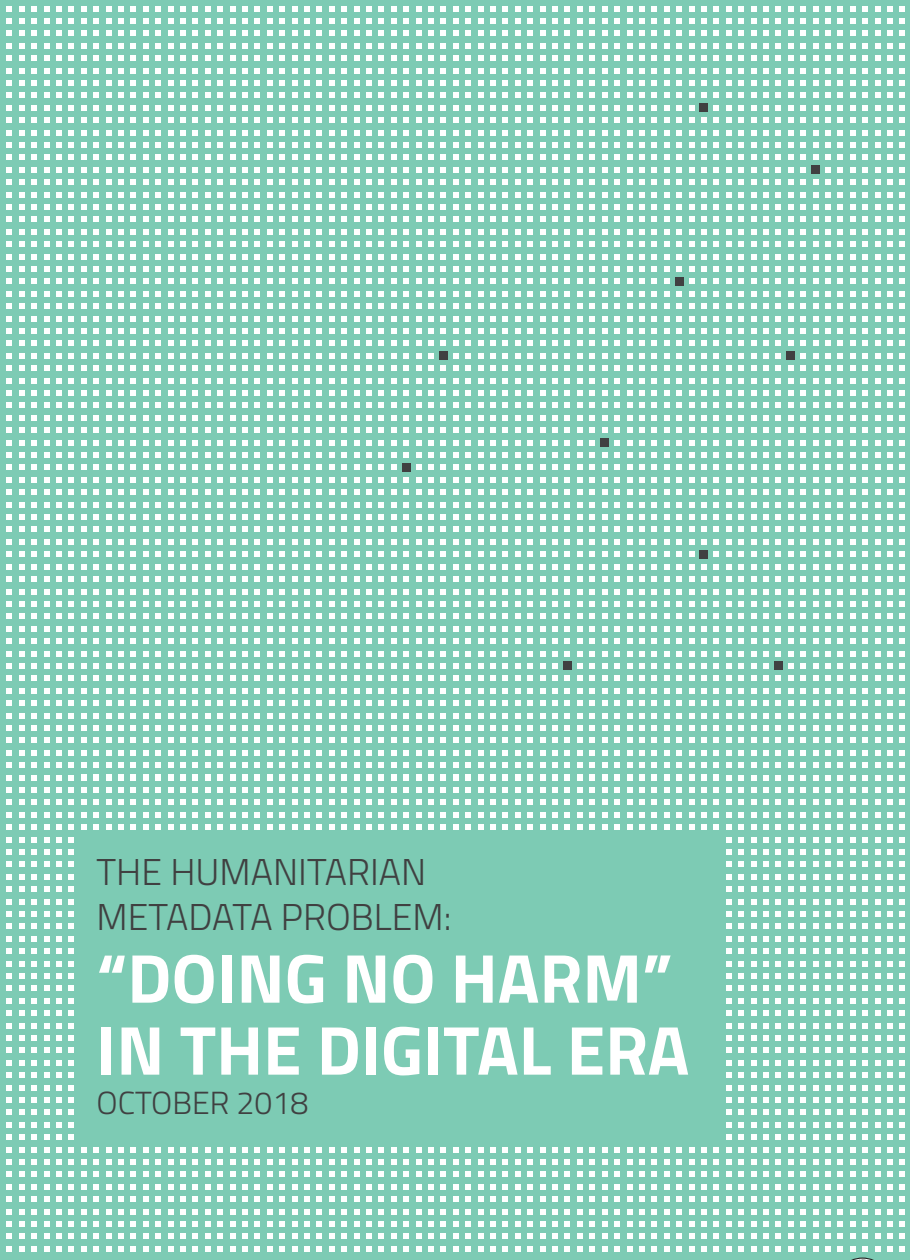


THE HUMANITARIAN
METADATA PROBLEM:

"DOING NO HARM" IN THE DIGITAL ERA

OCTOBER 2018

PRIVACY INTERNATIONAL

ICRC

THE HUMANITARIAN
METADATA PROBLEM:

"DOING NO HARM" IN THE DIGITAL ERA

OCTOBER 2018

About this study

New technologies continue to present great risks and opportunities for humanitarian action. To ensure that their use does not result in any harm, humanitarian organisations must develop and implement appropriate data protection standards, including robust risk assessments.

However, this requires a good understanding of what these technologies are, what risks are associated with their use, and how we can try to avoid or mitigate them. The following study tries to answer these questions in an accessible manner. The aim is to provide people who work in the humanitarian sphere with the knowledge they need to understand the risks involved in the use of certain new technologies. This paper also discusses the "do no harm" principle and how it applies in a digital environment.

This study was commissioned by the International Committee of the Red Cross (ICRC) to Privacy International (PI). The study does not advocate for privacy or against surveillance. Rather, it maps out where surveillance may obstruct or threaten the neutral, impartial and independent nature of humanitarian action.

This study is based on the most updated information publicly available and/or obtained by the authors at the time of writing (July 2018).

About the ICRC

The International Committee of the Red Cross (ICRC) is an impartial, neutral and independent organisation whose exclusively humanitarian mission is to protect the lives and dignity of victims of armed conflict and other situations of violence and to provide them with assistance.

The ICRC also endeavours to prevent suffering by promoting and strengthening humanitarian law and universal humanitarian principles.

About Privacy International

Privacy International is a registered charity based in London that works at the intersection of modern technologies and rights. It envisions a world in which the right to privacy is protected, respected, and fulfilled.

Privacy is essential to the protection of autonomy and human dignity, serving as the foundation upon which other human rights are built. In order for individuals to fully participate in the modern world, developments in law and technologies must strengthen and not undermine the ability to freely enjoy this right.

Acknowledgements

This study was written by Alexandrine Pirlot de Corbion, Dr Gus Hosein, Dr Tom Fisher, Ed Geraghty and Ailidh Callander, from Privacy International, and Tina Bouffet, from the ICRC. It also received written contributions from Jacobo Quintanilla, Massimo Marelli, and Silvia Pelucchi from the ICRC.

It was commissioned by Jacobo Quintanilla and Massimo Marelli and is the product of a collaboration between an advisory group and the authors.

The authors would like to sincerely thank all those who contributed to the general consultation process. They are particularly grateful to the members of the advisory group, who served in a personal capacity. Their input drew on the depth and diversity of their expertise and of the experience they have gained in their respective agencies and organisations.

The advisory group comprised the following members, in alphabetical order: Angela Onikepe (ICRC), Austin Shangraw (ICRC), Cheng Boon Ong (ICRC), David Arthur Brown (ICRC), Delphine van Solinge (ICRC), Gil Talon (ICRC), Heather Leson (IFRC), Jacobo Quintanilla (ICRC), John Warnes (UNHCR), Martin Searle (Nanyang Technological University, Singapore), Massimo Marelli (ICRC), Michael Herren (ICRC), and Ximena Contla Romero (ICRC).

Special thanks go to Sébastien Carliez and Philippe Stoll, whose unwavering support made this study possible.

This study does not reflect the official position of the ICRC, Privacy International, or any of the members of the advisory group. Responsibility for the information and views expressed in the study lies entirely with its authors.

The ICRC and Privacy International request due acknowledgement and quotes from this publication to be referenced as:

International Committee of the Red Cross (ICRC) and Privacy International, *The humanitarian metadata problem: "Doing no harm" in the digital era*, October 2018.

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

Table of contents

Foreword 9
Executive summary 11
Methodology 20
1. Introduction 21
1.1 What are metadata? 21
1.2 Surveillance today: a quick overview 22
1.2.1 How surveillance has evolved 23
1.3 Ten things you need to know 25
1.4 Why should the humanitarian sector care about metadata? 26
1.4.1 Privileges and immunities 26
1.5 Data for good: a double-edged sword? 30
2. Processing data and metadata 32
2.1 Declared data 34
2.2 Inferred and observed data 35
2.3 Interest and intent data 36
3. Threats when processing metadata 38
3.1 Understanding the legal and policy landscape 38
3.1.1 Governments' evolving access to metadata 39
3.1.2 How these surveillance capabilities are exacerbated 39
3.2 Stakeholders in metadata surveillance 40
4. Where services intersect 43
4.1 Messaging apps and social media 43
4.1.1 Case study: Facebook and WhatsApp 43
4.2 The financial and telecommunications sector 45
5. Telecommunications and messaging 46
5.1 SMS 47
5.2 Modern messaging protocols 50
5.2.1 CryptCorp Fictional Case Study 52
Part 1. SSL/TLS tunnels 52
Part 2. "Man-in-the-middle" attacks 54
Part 3. Domain fronting 56
Part 4. State restrictions 58
5.2.2 Real case studies 58
5.3 Other metadata 60
5.4 Outsourcing, contracting, and using third parties 63
5.5 Ad networks and tracking 64

6. Cash-transfer programmes (CTP) 66
6.1 CTP and financial inclusion: benefits and challenges 68
6.2 Analysing cash-transfer programming 70
6.2.1 Mobile money 70
Data held by a domestic service provider 71
6.2.2 Banking 77
Data held by CTP recipient's bank 77
Other organisations 79
Scenario C 82
Smartcard providers 83
Scenario D 84
7. Social media platforms 85
7.1 The humanitarian sector's use of social media platforms and data 85
7.2 Social media platforms and data 92
7.2.1 Facebook 92
Data 93
Facebook "Apps" 96
7.2.2 Twitter 96
Data 96
7.3 Social media metadata 99
7.3.1 Monitoring social media data 99
Open source intelligence (OSINT) 99
Social media intelligence (SOCMINT) 100
Public vs private data 102
7.3.2 Usage of Android apps & permissions 103
7.4 Unregulated uses of social media (meta)data 105
7.4.1 Financial sector 106
7.4.2 Predicting personal attitudes and traits through data and metadata 106
7.4.3 Political campaigning 107
7.5 Key considerations: the use of social media by humanitarian organisations 108
8. Conclusion 110
Glossary 112
Bibliography 114
Court Cases 127

Foreword

The digital era is enabling spectacular advances in the field of humanitarian action. It makes it possible to improve the effectiveness and efficiency of aid provision in regions affected by war or disaster. The use of technology – including smartphones, drones and other connected objects – can provide more relevant responses to the expectations and needs of local communities. Meanwhile, social networks can play a crucial role in information and awareness-raising campaigns, and as a means of communication and information disclosure.

However, the use of these technologies also leaves traces. It can allow for the tracking and profiling of individuals, with great risk to their lives, integrity and dignity. This applies regardless of whether the individual is seeking humanitarian aid or providing it as a humanitarian staff member or volunteer. Already, the data generated by the humanitarian sector has stirred up interest within certain governments, groups and intelligence agencies, at the risk of undermining the impartiality, neutrality and independence that organisations like the ICRC must demonstrate.

This study by Privacy International and the ICRC on the issue of humanitarian metadata represents a valuable complement to the Handbook on Data Protection in Humanitarian Action, which the ICRC published in July 2017. It also furthers the organisation's efforts to ensure a high level of data protection when using information and communication technologies. Finally, it provides relevant insights into the use of different technologies and the inherent risks that they entail.

I hope that this report will raise the humanitarian community's awareness of this issue and of their responsibility and obligations in terms of data protection and security. Above all, I hope it will help them take the necessary measures to prevent ill-intentioned third parties from accessing data held by humanitarian organisations, and safeguard the impartiality, neutrality and independence of humanitarian action in an ever-growing digital space.

Jean-Philippe Walter
Swiss Deputy Federal Data Protection
and Information Commissioner

Executive summary

Introduction

Background

The past decade has seen a surge in the use of mobile telecommunications, messaging apps and social media. As they become more accessible around the world, these technologies are also being used by the humanitarian sector to coordinate responses, communicate with staff and volunteers, and engage with the people they serve.

These exchanges lead to an increase in metadata: data about other data. In their most common form, metadata are the data that are generated around a message, but not the content of the message. Imagine that you are a clerk at the post office: content data would be information contained *inside* each parcel that comes your way. These content data are often protected by law and other technical safeguards. However, metadata – data that are found on the *outside* of the parcel or that can be inferred from the parcel's appearance – are often less well protected. They can be accessed and read by third parties as they pass through the postal system.

What are metadata?

Today there are many forms of such data. In this report, we differentiate between declared data, inferred data, and interest or intent data. These data can be owned, processed, shared and stored for different periods of time, by different third parties, and under different jurisdictions applying different regulations.

This complex landscape requires that humanitarian organisations learn how to more systematically assess, understand, and mitigate the risks involved in programme activities that generate metadata.

Main findings

Why should the humanitarian sector care about metadata?

Humanitarian organisations collect and generate growing amounts of metadata. They do this through their exchanges internally and with people affected by crises (e.g. sharing "info-as-aid" over messaging apps and/or via SMS and social media); their programmes (e.g. cash-transfer programmes that use mobile cash or smartcards); and their monitoring and evaluation systems (e.g. using data analytics on programme data to detect fraud).

To reconcile these actions with the "do no harm" principle, the humanitarian community must better understand the risks associated with the

generation, exposure and processing of metadata. This is particularly important for organisations that enjoy certain privileges and immunities but that are not able to counter these risks alone.

Processing data and metadata

Specifically, humanitarian organisations need to better understand how data and metadata collected or generated by their programmes, for humanitarian purposes, can be accessed and used by other parties for non-humanitarian purposes (e.g. by profiling individuals and using these profiles for ad targeting, commercial exploitation, surveillance, and/or repression).

For instance, information about an individual registered for a cash-transfer programme can be accessed and used by the financial institution implementing the programme. The institution can then use this information to categorise the individual as a non-trustworthy borrower, thereby limiting their access to financial services. If the institution has information-sharing agreements with other institutions that are part of the same financial group, this sort of profiling can prevent the individual from accessing those institutions' services as well.

Understanding the legal and policy landscape

To fully appreciate such situations, humanitarian organisations should map out who exactly has access to the data and metadata they generate and for how long. These factors are affected by the technical, legal and policy landscapes, which vary greatly despite efforts to streamline regulations (through initiatives like the EU's General Data Protection Regulation, for example).

These landscapes are also changing as expanded access to data is sought by both public entities (e.g. to combat crime or follow migration flows) and private ones (e.g. to monetise user data or improve their business models). Moreover, some service providers may have an obligation to disclose data or metadata. For instance, a number of banks are obliged to flag "suspicious activity" on their client's accounts or collect information about clients under Know Your Customer regulations designed to prevent money laundering and other criminal activity.

Where services intersect

The following section summarises the risks associated with the use of traditional telecommunication services (including voice and SMS), messaging applications, cash-transfer programming and social media. While each type of service is discussed separately, they may overlap where financial companies are also telecommunication companies or where social media providers also own messaging applications. This has implications for the amount of data and metadata any given entity has access to or can generate and for the variety of jurisdictions under which these data are generated and stored.

Identified risks & recommendations

Telecommunications and messaging

Today's 2G, 3G and 4G mobile networks actually describe a series of protocols that operate over different frequencies, using different encryption algorithms, and allowing different speeds. Even with the gradual rollout of 4G or LTE for data connections, most carriers still revert to the much less secure 2G protocol for voice and SMS communications. This means that the metadata and content of telecommunications are still at risk of being intercepted between a given phone and the phone tower routing the communications. Moreover, telecommunication networks were not designed to deliver emergency-scale loads of SMS traffic – hence the high failure rates when the network is saturated. This calls into question the recommended use of SMS campaigns in crisis situations.

Risks. When using telecommunications, humanitarian organisations put all parties involved at risk of their telecommunication data (message or call content) being intercepted and the associated metadata (sender/recipient, time and location) being accessed. Even when calls or messages are not being exchanged, mobile phones regularly "ping" nearby cell towers to ensure the best possible continuous service. As a result, users can be tracked through their phones' location service. This tracking continues even when the phone is not being used, is in sleep mode, or is turned off.

Mitigation. End-to-end encrypted, secure communication methods should be used instead of voice or SMS even if they do not always prevent metadata from being accessed. Even with the stronger encryption of VoLTE (Voice over LTE), downgrade attacks (which force the device to switch to a less secure encryption method) are possible. These less secure encryption methods only work between the phone and the tower. Until there is more widespread and routine use of end-to-end encrypted communications that minimise metadata, humanitarian organisations should conduct advance risk assessments for all telecommunications exchanges; here, they should always plan for scenarios in which third parties are able to gain access to the content, time and location of all exchanges.

Messaging Apps

Messaging apps use a number of different encryption algorithms with varying levels of transparency as to how that encryption is integrated in the app. In many cases, encryption is only applied to specific types of communications on the app (e.g. when communications are set to private mode). Encryption methods include end-to-end encryption: if SMS messages are like postcards, where everything can be read, messaging apps are like envelopes where only the destination and sender can be seen by the local provider. They also include SSL/TLS tunnels, a rough

equivalent to putting another envelope around the first, and marking the messaging platform – e.g. WhatsApp – as the destination. Finally, there is also a now defunct method called domain fronting: if the messaging application was banned in a particular location, domain fronting allowed the app provider to put a third envelope around the first two and write the name of a permitted domain on it. These domains were often deemed too large to ban outright (e.g. Google or Amazon). However, some of these methods are still susceptible to attacks – like a man-in-the-middle attack, where a third party poses as the messaging platform to the user and as the user to the messaging platform, in order to intercept exchanges. Whilst many messaging apps will automatically prompt users if another party's encryption key changes (which could indicate a man-in-the-middle attack or, alternatively, the user using a new phone), most users have been trained to click "Ok" to prompts and error messages. This entirely bypasses the added security that this would otherwise provide.

Risks. While some messaging apps encrypt message content during communications, they also commonly ask the user to reveal more data, share more data than the user may realise (such as the device and SIM identifiers – IMSI and IMEI – and information on the phone), or ask the user to give the app permission to access other information on their device such as location, photos and contacts. This allows the messaging app provider to gather extensive information on the user over time. For instance, a messaging app could infer – from the frequency of your calls or SMS communications – when you wake up, go to sleep, what time zone you're in, and who your closest friends are.

Mitigation. Humanitarian organisations could discuss how to increase data and tech literacy among staff, volunteers and crisis-affected people when messaging apps are used to communicate. This would allow these users to make informed decisions about what information they share on what platforms. Risk assessments for the use of messaging apps should also take into account not only what data has to be declared by the user, but what can be inferred over time, depending on the device information that apps can access. Messaging apps can also share information among themselves if they are run by the same provider or in the same app library. This makes it all the more important to map out who has access to what data, under which jurisdiction. Finally, the humanitarian community could explore what leverage they have to negotiate greater protection or discretion from messaging app providers in certain situations.

Cash Transfer Programmes

In cash-transfer programmes (CTP), humanitarian organisations provide cash or vouchers directly to crisis-affected people. CTP's growing use of digital and telecommunication technologies has enabled greater financial inclusion. However, these third-party technologies also make it easier for

the individuals registered to be identified. Their increased digital visibility creates risks of discrimination and persecution.

Mobile Money

Mobile money refers to the use of mobile wallets, where funds can be transferred using a mobile-phone-based system. This CTP delivery method does not require a bank account, but it does rely on third-party domestic telecommunications companies.

Risks. Mobile money transaction details are often reported to the recipient via an unencrypted SMS. Thus, even when the electronic transfer is encrypted, the details of the transaction are not and can be intercepted directly or by other apps on the recipient's phone. Moreover, the domestic telecommunications company may be obliged (e.g. by Know Your Customer regulations) or inclined (e.g. for their commercial partnerships) to share data collected or inferred from the CTP. These data can be used to financially profile a person, and this may restrict their access to financial services in the future.

Mitigation. The use of mobile money should be preceded by the same type of risk assessment proposed for telecommunications. Because the use of CTPs is strongly associated with humanitarian programmes, organisations should take steps to ensure that persons registered in these programmes are not automatically associated with specific identity factors. For instance, in a situation where a minority group is being persecuted, humanitarian organisations should be wary of launching a CTP that they know will only attract people from that group. Rather, a wide variety of people should be registered, as this will prevent the CTP participant list from becoming an indirect census of that group. Finally, humanitarian organisations should also check who owns/controls the telecommunications operations involved in a CTP. This may reveal useful information on how the company operates and what additional threats or risks there may be regarding data sharing (e.g. if the company has an incentive to share data with the host government, which could be undesirable).

Banking

Some CTPs require that individuals set up a bank account or use an existing one. The involvement of the banking sector means that access to personal information can be extended to third parties like national anti-corruption and financial intelligence bodies, other banks from the same banking group, intermediary banks, credit bureaus and credit rating agencies. Moreover, banks usually require a significant amount of information to set up an account (e.g. under Know Your Customer regulations). Using these data along with transactional metadata, they are able to infer a large amount of information about their clients (such as periods of informal employment and political and religious leanings).

Risks. As mentioned above, depending on the bank's regulatory framework and broader partnerships, individual data collected through a CTP can be shared with other parties, both domestic and international. These data can be used to create and monitor an individual's credit profile, with potential repercussions on their access to credit; to track their movements across borders (e.g. in the case of international banking groups); or to discriminate against them on the basis of inferred political or religious affiliations.

Mitigation. When selecting the bank for a CTP, humanitarian organisations should map the country's data-sharing laws and practices as well as the bank's ownership, partnerships and information-sharing agreements. They should also try to negotiate a "no sharing" agreement for CTP data and limit the data retention period to ensure that CTP data will not be automatically stored for decades after the programme has ended.

Smartcards

Smartcards are similar to electronic wallets in that they can be used to transfer and spend cash. Their electronic chip links the wallet to a specific owner and keeps track of the account balance. Each smartcard transaction generates a record that is geo-located and time-stamped and that includes the transaction amount. It also keeps a record of the payment terminal used to process the transaction, the shop itself, and, in some cases, the items purchased.

Risks. Smartcard metadata are usually sufficient to identify an individual with a high degree of precision. Behavioural patterns, physical movements, and purchasing habits can then all be inferred and attributed to the identified individual(s). Should these data become accessible to a third party, e.g. when shared with an external firm for programme evaluation, they can be used to track and persecute vulnerable groups (e.g. refugees participating in a CTP).

Mitigation. When designing a smartcard-based CTP, humanitarian organisations should map out all the entities involved in the process (e.g. smartcard provider and bank) and any other partners or entities that can access their data. Organisations should also try to negotiate a limit on the amount of data needed to set up the programme and whether the metadata involved (e.g. geo-location) can be excluded from the data-handling process. Finally, they should discuss the retention period and the ability of third parties to access these data.

Social media

Social media have become a ubiquitous tool of user engagement. Their expanding functions now include services specifically tailored to crisis situations, such as Facebook's Disaster Maps. However, social media

providers' business model still relies on the monetisation of user data (e.g. for ads targeting). This means that social media data, even if they are gathered for humanitarian purposes, are vulnerable to the same level of commercial exploitation as any other data on Facebook, Twitter, etc.

This issue is further complicated by the ever-changing nature of social media providers' privacy and data protection policies. Users often have little or no say in accepting these updates (i.e. they must either accept the update or deactivate/delete the account). The abundance of information that can be obtained, inferred or derived from social media data has generated great interest in social media intelligence (SOCMINT). Indeed, SOCMINT has become increasingly popular with both private and public parties for surveillance and other non-humanitarian objectives. Meanwhile, it is very difficult for users to know which data are being generated and processed by the platforms they use; which actors have access to these data (each social media platform has its own policy on transparency reporting); and what the regulatory environment is.

Risks. Using the large amount of data and metadata generated on social media, it is possible to very accurately predict people's behaviour, preferences, and other personal details (e.g. ethnicity, sexual orientation and political and religious affiliations). But it can also lead to erroneous inferences, if the original data or any other data used for correlation purposes were inaccurate or biased. Users' data and metadata are usually saved in a "shadow profile" that can be accessed, sold, and freely shared with third parties. These profiles can be exploited for surveillance purposes and to attempt to influence users' behaviour (as suggested by the 2018 Cambridge Analytica controversy). Often, even if a user deletes a given social media account, limits the number of apps that can access it, or never had an account in the first place, their shadow profile exists and is fed by information gleaned from other social media accounts or websites they use and even from their contacts' social media accounts (e.g. their Facebook friends).

Mitigation. To appreciate the risks involved in social media metadata, humanitarian organisations should increase the digital literacy of their staff and volunteers and of the people they serve. Emphasis should be placed on the business model employed by the various social media platforms in order to then asses their threat model and risk appetite. They should also carry out risk assessments to understand what individual or group vulnerabilities may be exposed if the organisation uses social media for a particular activity. Finally, the sector as a whole could jointly negotiate with major social media platforms (e.g. Facebook and Twitter) in order to secure specific safeguards across their services and in particular for humanitarian metadata.

Background

In 2013, Privacy International published "Aiding Surveillance",[1] a report that raised concerns around development and humanitarian organisations' adoption of new technologies and data-intensive systems (e.g. biometric identification schemes). Specifically, the report revealed how these systems and technologies enabled and facilitated the surveillance and repression of people who register to benefit from development and humanitarian programmes. It also stressed how the personal data and information generated by these programmes were subject to few legal safeguards. This presented serious threats to individuals' human rights, and particularly their right to privacy.

In January 2017, the ICRC, The Engine Room and Block Party produced a report called *Humanitarian Futures for Messaging Apps. Understanding the Opportunities and Risks for Humanitarian Action*.[2] The report highlighted how the widespread use of messaging apps may warrant their "strategic" use in humanitarian operations. Indeed, messaging apps can play a key role in sharing vital information with or among people affected by crises, in documenting events, or in combating misinformation.

However, the use of messaging apps can also entrench old inequalities or create new ones along digital, age and gender divides. Their use also raises an important number of concerns around security, data protection, privacy, and consent.

The report also included discussions on metadata: or, data that describe other data. Metadata can include the time or location at which a message was sent, but doesn't include the message content itself. By their very nature, most mobile messaging apps collect, store, and generate various types of metadata, both on the device itself and on the networks and services used. These metadata could be accessed and exploited by unauthorised third parties, including people or entities involved in conflict and violence or private companies. This could threaten the safety of those involved in humanitarian programmes, especially where metadata are used for purposes that run counter to the neutral, impartial and independent nature of humanitarian work.

1 Gus Hosein and Carly Nyst, "Aiding Surveillance: An Exploration of How Development and Humanitarian Aid Initiatives Are Enabling Surveillance in Developing Countries," *SSRN Electronic* Journal, Privacy International, October 2013, https://privacyinternational.org/report/841/aiding-surveillance.

2 Tom Walker, "Humanitarian Futures for Messaging Apps – Understanding the Opportunities and Risks for Humanitarian Action" (ICRC, The Engine Room, Block Party, January 2017), www.icrc.org/en/document/messaging-apps-untapped-humanitarian-resource.

Similar concerns were raised in the ICRC and Brussels Privacy Hub's *Handbook on Data Protection in Humanitarian Action*.[3] The Handbook underlined how humanitarian organisations' growing reliance on digital intermediaries – be it for communication and outreach, cash and fund transfers, or data analytics – gives rise to "humanitarian metadata". In this context, the onus is on humanitarian organisations to recognise and act on their duty of care towards the people they seek to protect and assist.

The present study aims to help humanitarian organisations fulfil this duty of care. By exploring the risks associated with metadata, it can inform evidence-based risk assessments and monitoring. It can then help identify whether these risks can be accepted, transferred, controlled, avoided, or mitigated at their point of inception or at any other point.

3 Christopher Kuner and Massimo Marelli, eds., *Handbook on Data Protection in Humanitarian Action* (ICRC, Brussels Privacy Hub, 2017), www.data-protection-handbook.icrc.org.

Methodology

This study is based on a review of the relevant literature and interviews with representatives of the humanitarian sector. These include headquarters and field staff from non-governmental and humanitarian organisations and United Nations agencies, together with academics who identify as members of the tech community and civil society. All interviewees were selected by the ICRC, the authors, the advisory group and other contributors.

Efforts were also made to reach out to the global service providers referred to in this study.

Limitations

The views of the individuals interviewed for this study do not necessarily represent the views of everyone who works in the humanitarian sphere or their organisations. However, the interviewees were carefully selected so as to provide a range of opinions and experiences relating to the subject of the study. Due to the study's limited scope, no interviews were carried out with people affected by crises.

The study's authors submitted multiple requests to global service providers for more information on their technologies and practices; none of these requests were answered. In the absence of this information, the study drew on what is known publicly and through the literature and/or primary data analysis.

It is worth noting that the companies mentioned in this study may change their services and general terms and conditions at any point in time. This can affect the level of metadata generated, how metadata are processed, and leakage. Government agencies' executive powers and the legal environment in which they function may also change as interest in "fake news", data protection and access to information is on the rise.

SECTION 01

Introduction

METADATA
pl.n. *(used with a sing. or pl. verb)*
Noun: metadata; noun: meta-data
A set of data that describes and gives information about other data.

1.1 What are metadata?

Let's imagine you work at the post office. Every day, you receive packages. For each package, you note the return address, the date it arrived, and the person to whom it is addressed. Moreover, you might have a vague idea of what the package contains based on the company who sent it. Given the wrapping and the time of the year, you might also infer that it's a gift. All in all, you were able to get a lot of information about this package – without ever opening it.

Now, let's imagine that you're a telephone operator. It's late at night, and you're asked to connect a hospital's emergency room to the president's personal phone line. Between the recent headlines you've read in the press and the brevity of the phone conversation, you're able to guess the kind of news that's just been shared.

Neither scenario involved any eavesdropping or device tampering. All the information you obtained – the metadata – was consequent to the communication itself. These metadata were made accessible to you, a third party, without the say of the individuals involved. This was an inevitable result of the communication simply taking place: the content of people's interactions was revealed by correlating observed metadata, legally obtained through their use of an intermediary platform. At no point was any right to privacy explicitly forfeited.

1.2 Surveillance today: a quick overview

"We kill people based on metadata."

- Statement by General Michael Hayden, former director of the United States National Security Agency and of the Central Intelligence Agency, May 2014.

General Hayden's comment in the spring of 2014 was the first to articulate the power of metadata so succinctly and famously.[4] It wasn't so much that metadata could reveal information – that much had always been known. It was the extent to which this information was both trusted and used to make life-and-death decisions.

In the years that followed, more information emerged on the breadth and scope of global intelligence agencies' mandate, functions, operations, and oversight (or lack thereof). Some agencies were listening in on calls, monitoring or intercepting online communications, and tracking individuals through a variety of digital and non-digital programmes.[5]

In doing so, they were able to access metadata that could tell them what they wanted to know about a situation: who was involved, where they were, and when, how and with whom they were interacting. For these agencies, the advantage of metadata is that they leak: they are easily observable all along the chain of communication that they describe. It is almost impossible to prevent metadata from being generated; or to obfuscate or hide them after the fact.

This allows metadata to be processed on a massive scale or combined with other (meta)data sets in order to generate new information. This information can be more reliable than that provided by humans. Indeed, while an individual may enter inaccurate information in a message, the message's metadata will accurately reveal details like the device location, the time the message was issued, the message recipient, and any other information required by the relevant protocol.

To prevent this, some might suggest using access controls or encryption. However, getting a message from one location to another usually requires

4 David Cole, "We Kill People Based on Metadata," *The New York Review of Books,* May 10, 2014, Online edition, sec. Daily, http://www.nybooks.com/daily/2014/05/10/we-kill-people-based-metadata/. Watch the full conference here: Johns Hopkins University, *The Price of Privacy: Re-Evaluating the NSA,* The Johns Hopkins Foreign Affairs Symposium, 2014, https://www.youtube.com/watch?time_continue=1022&v=kV2HDM86XgI.

5 See: Privacy International, "Communications Surveillance," Privacy International, n.d., https://privacyinternational.org/topics/communications-surveillance; "Privacy and Surveillance," ACLU, n.d., https://www.aclu.org/issues/national-se curity/privacy-and-surveillance.

multiple entities knowing its source and destination. In other words, some metadata are shared by necessity. As a result, a growing number of logs are created by default: arrivals and departures, deposits and withdrawals, "likes" and visits. These logs are accessible to those involved in the communication chain.

However, they are also increasingly accessed – lawfully or unlawfully – by third parties interested in the activities, intentions and personal profiles that can be inferred from them. Such analyses are facilitated by constant advances in data analytical tools and processing power and storage, which together allow ever greater quantities of metadata to be generated, stored, and analysed.

1.2.1 How surveillance has evolved

Surveillance today can be carried by governments, lawfully or not, and by corporations that take advantage of the services they provide to gather, process, or infer information. Over the past 25 years, these two types of surveillance have transformed dramatically due to four dynamics:

First, the ongoing improvement in data processing capabilities. Governments and other interested parties have access to software and hardware that make it easier and cheaper to collect, analyse and store metadata and to generate intelligence.

Second, there are growing amounts of data and metadata that can be processed. The rise of digital – i.e. mobile and internet – communications has massively increased the amount of data and metadata that we generate or that are generated about us (whether we know it or not). And it can all be used for surveillance purposes.

These evolving dynamics became most apparent after 9/11. Around the world, governments passed laws demanding broader access to communications metadata. For instance, the British Government requested access to all metadata generated within its borders.[6] Authorities also purchased

6 See: Ben Wagner, *After the Arab Spring: New Paths for Human Rights and the Internet in European Foreign Policy,* Directorate-General for External Policies of the Union (Luxembourg: European Parliament, 2012), http://bookshop.europa.eu/uri?target=EUB:NOTICE:BB3212238:EN; Jillian C. York and Trevor Timm, "Surveillance Inc: How Western Tech Firms Are Helping Arab Dictators," *The Atlantic,* March 6, 2012, Online edition, https://www.theatlantic.com/international/archive/2012/03/surveillance-inc-how-western-tech-firms-are-helping-arab-dictators/254008/; Privacy International, "Middle East and Northern Africa," Privacy International, https://www.privacyinternational.org/location/middle-east-and-northern-africa; "BAE Sold Surveillance Tools to Arab States," *BBC News,* June 15, 2017, sec. Middle East, https://www.bbc.com/news/world-middle-east-40276568.

various surveillance technologies[7] and set up domestic and global surveillance programmes dedicated to metadata.[8] Once disclosed to the public, these decisions revealed not only governments' mounting surveillance capabilities, but also the evolving breadth and scope of the policies and practices under which they operate.

Third, more of our actions and interactions now generate data and metadata. The act of communicating is no longer a prerequisite. When we visit a website, a log is generated. If we read an article on that website, a further log is generated. When we see a 'like' button on a webpage, we know that metadata are being shared with a social media company. Our movements can be communicated by our mobile devices; our financial interactions, by the device we used, the bank accounts involved, or other intermediaries (e.g. the mobile application used). Even our phone's battery level can be traced and used to infer conduct and behaviour.[9]

This phenomenon is linked to the rise in mobile applications that help people to engage with their world – book a hotel, pay for a service, travel, or track their athletic performance. These applications gather and monetise new kinds of data, many with little or no regard for people's privacy.

Finally, metadata surveillance no longer concerns itself with the individual. Today's processing and storage capabilities mean that entire groups, populations, or regions can be placed under surveillance. Their movements, types and rates of interaction, use of services, and any other indicators of behavioural change can be invaluable sources of information for companies and intelligence agencies. To understand this, one must first look at how metadata are generated and processed and what information can be drawn or inferred from them.

7 Glenn Greenwald, Ewen MacAskill, and Laura Poitras, "Edward Snowden: The Whistleblower behind the NSA Surveillance Revelations," *The Guardian*, June 11, 2013, sec. US news, http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance.

8 Ibid.

9 Andy Greenberg, "Spies Can Track You Just by Watching Your Phone's Power Use," *Wired*, February 19, 2015, Online edition, sec. Security, https://www.wired.com/2015/02/powerspy-phone-tracking/.

1.3 Ten things you need to know

1. **Metadata are unintentional consequences of an interaction.** Nearly every interaction on a technological device or using technology generates metadata for all users and entities involved in the transaction.
2. **Encryption rarely secures metadata.** Encryption may secure the *content* of communications, but metadata will at the very least still reveal *who* is performing the transaction. At best, encryption may reduce the number of stakeholders that have access to the metadata.
3. **The data contained in your device's applications may not be encrypted.** These applications can also access other data on the device, without your knowledge or consent, such as the device and SIM identifiers (IMEI and IMSI) and the battery level.
4. **Often, your device's data are unencrypted.** This is particularly true for older Android devices, as well as lower-cost devices that are either running legacy operating systems or don't have the hardware capability for encryption.
5. **Governments are increasingly seizing and accessing devices.** This can grant them access to huge amounts of data (including metadata), content that would be encrypted when in transit, and deleted data.
6. **Providers can (and usually do) generate data on any activity or actor involved** from the moment the providers act as an intermediary for that activity.
7. **Individual data can be purchased by service providers from other parties**. These data may concern people on whom the providers previously had no data, or the purchased data can increase the size of the providers' existing records.
8. **Providers can grant other entities full or partial access to their data or metadata.** This is commonly referred to as the commercial exploitation of data, and it often occurs without the individual concerned being informed.
9. **To date, the best way to prevent metadata being generated is to not interact at all.** Metadata privacy services have yet to be sufficiently explored or adopted to curtail the generation of humanitarian metadata as discussed in this report.
10. **This state of affairs serves the purposes of a number of influential entities,** which means that changing the situation will require effort.

1.4

Why should the humanitarian sector care about metadata?

The relationship between humanitarian organisations and crisis-affected communities used to involve relatively few data. However, the spread of mobile and internet technologies has changed the way the two sides interact with each other. Today, new platforms are being used by different actors with different levels of understanding, agency and expectation. This gives rise to new relationships that are increasingly shaped by technology – both positively and negatively.

In this convoluted ecosystem, the humanitarian sector uses and generates metadata. The sector also causes more metadata to be generated by encouraging people to use certain devices or services (e.g. messaging apps, cash-transfer programmes). This means that humanitarian organisations both drive and depend on data generation and data processing. They also infer information and intelligence about individuals.

To reconcile these actions with the "do no harm" principle, the humanitarian community must better understand how its use of technology – even for laudable purposes – might end up undermining the rights and safety of the people they are seeking to help. Indeed, by simply interacting with someone over social media, a humanitarian organisation can create unwanted associations for that person and expose them to specific vulnerabilities, depending on the context, type of interaction, type of organisation, and other available datasets.

1.4.1 Privileges and immunities

Some humanitarian organisations with international status enjoy specific privileges and immunities. These privileges and immunities help to ensure that an international organisation is able to fulfil its mandate in full independence, and – where applicable – in compliance with the principles of humanity, impartiality and neutrality. It also enables them to act without interference from parties to a conflict or actors in other situations of violence.

During humanitarian emergencies, these privileges and immunities may have value as a first line of protection for affected people's personal data. This was recognised in the Resolution on Privacy and International Humanitarian Action issued in 2015 by the International Conference of Privacy and Data Protection Commissioners.[10] Specifically:

> *"Humanitarian organisations not benefiting from Privileges and Immunities may come under pressure to provide data collected for humanitarian purposes to authorities wishing to use such data for other purposes (for example control of migration flows and the fight against terrorism). The risk of misuse of data may have a serious impact on data protection rights of displaced persons and can be a detriment to their safety, as well as to humanitarian action more generally."*[11]

Even in the presence of privileges and immunities, the protection of affected people's personal data can be jeopardised or weakened whenever a humanitarian organisation's activities involve a third-party service provider. This is because the service provider does not enjoy the same privileges and immunities and is subject to the jurisdiction of parties that may be interested in gaining access to the data.

The service provider might also disclose, not only the personal data of a specific person, but metadata regarding that person's interactions with humanitarian organisations (e.g. time and frequency). These metadata can be used to infer or generate new intelligence about a person or community.

The mere act of labelling someone an "affected person" also presents risks. Individuals who interact with humanitarian organisations might be profiled as vulnerable or sensitive. Depending on the situation, the cause of this vulnerability might be easily – although not always correctly – inferred (for example, by assuming that someone's vulnerability is the result of belonging to a particular political group).

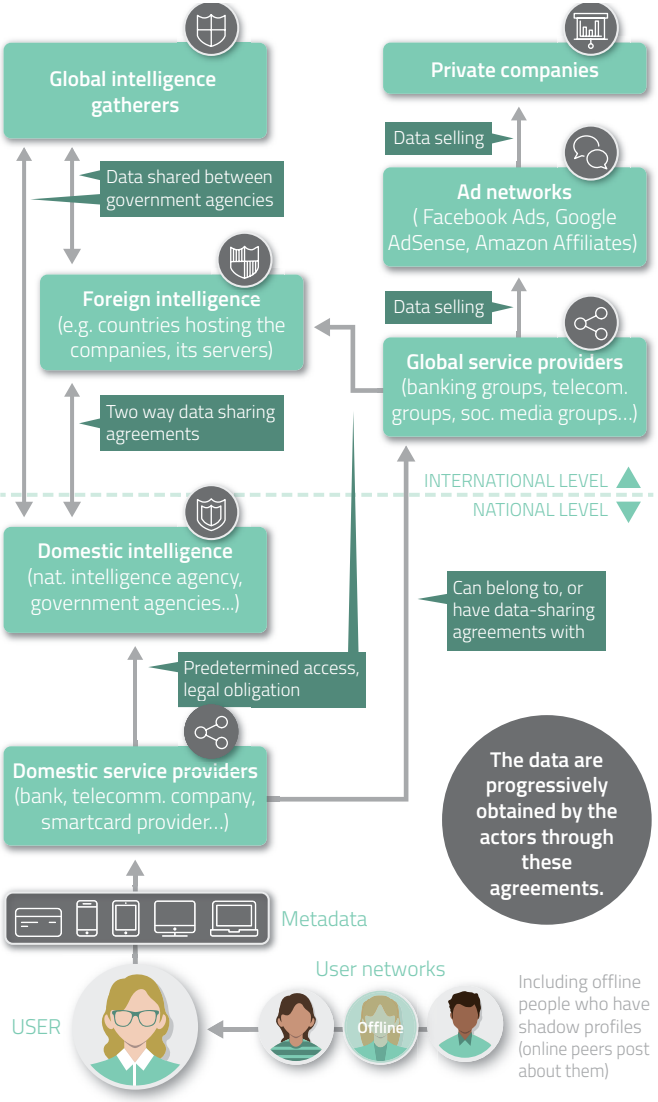
This allows metadata to forever mark an individual for exploitation or discrimination. Their simple interaction with a humanitarian organisation can hamper their access to future banking services or expose them to targeted advertising for financial products with high interest rates.

10 "Resolution on Privacy and International Humanitarian Action," in *37th International Conference of Data Protection and Privacy Commissioners* (Amsterdam, 2015), https://icdppc.org/wp-content/uploads/2015/02/Resolution-on-Privacy-and-International-Humanitarian-Action.pdf.

11 Ibid.

DIAGRAM 01

Who has access to what, and from where



The humanitarian sector itself is also a surveillance target. In 2013, journalists reported that a list obtained from whistle-blower Edward Snowden included UNICEF, Médecins du Monde, UNDP, and other agencies as surveillance targets for British and American intelligence agencies.[12] Further investigations subsequently determined that the British government had used signals intelligence (SIGINT) capabilities to unlawfully retain metadata from Amnesty International.[13]

Why are intelligence agencies interested in humanitarian organisations? Because of the places where humanitarian organisations operate. These areas are often experiencing conflict or social, economic or political instability. Their vulnerability can be construed as a threat to national security, prompting the agencies to collect relevant metadata in order to monitor the situation.

As the humanitarian sector digitalises more of its processes and involves more third-party service providers, it also generates growing amounts of metadata. These providers all produce them: banks, for cash transfers; telephone operators, for SMS campaigns; and internet access providers, for digital messaging applications. Some metadata are consciously collected by the humanitarian organisations themselves for monitoring purposes (e.g. keeping a list of cash-transfer recipients). Others are collected automatically and might be used or sold by a third party provider, without the organisation's knowledge, for advertising or profiling purposes.

12 Leigh Daynes, "Doctors of the World: How We Discovered GCHQ Was Spying on Us," *OpenDemocracy*, April 20, 2015, Online edition, https://www.opendemocracy.net/digitaliberties/leigh-daynes/doctors-of-world-how-we-discovered-gchq-was-spying-on-our-operations; James Ball and Nick Hopkins, "GCHQ and NSA Targeted Charities, Germans, Israeli PM and EU Chief," The Guardian, December 20, 2013, sec. UK news, http://www.theguardian.com/uk-news/2013/dec/20/gchq-targeted-aid-agencies-german-government-eu-commissioner.

13 Investigatory Powers Tribunal (IPT), Determination [2015], UKIPTrib 13_77-H_2, Case N.: IPT/13/77/H, IPT/13/92/CH, IPT/13/168-173/H, IPT/13/194/CH, IPT/13/204/CH, London, 22 July 2015, para. 14; Privacy International, "GCHQ Unlawfully Spied on Amnesty International, Court Admits," Privacy International, July 1, 2015, http://privacyinternational.org/press-release/1156/gchq-unlawfully-spied-amnesty-international-court-admits.

1.5 Data for good: a double-edged sword?

"Data for good" refers to the idea that data can be used as a tool to accelerate development, reduce poverty, spur innovation, and improve accountability and transparency. Promoting this concept are organisations like UN Global Pulse, the UN Economic Commission for Latin America and the Caribbean, the OECD, and the World Economic Forum.

In 2014, a report by the UN High Level Panel on the Post-2015 Development Agenda called for a "New Data Revolution", where existing and new sources of data would be used "to fully integrate statistics into decision making; promote open access to and use of data; and ensure increased support for statistical systems."[14]

To a certain extent, the humanitarian sector has also embraced this data revolution, recognising the future as digital and data-driven. To boost effectiveness and efficiency, it has adopted and promoted data-intensive technologies and systems. These technologies and systems have, under the aegis of "data for good", offered insights into the characteristics, behaviours, interests, and possibly intents of affected persons.

Such data are valued by researchers, humanitarian organisations, and funders alike. For humanitarian organisations specifically, these data can help them to identify and locate people at risk, share information with them, coordinate subsequent activities in the field, and gather feedback to improve programming. This last point aligns with a broader push to make humanitarian organisations "more client-focused", using data "to support a new generation of service delivery focused around the needs of their clients, customers, and constituents."[15]

These efforts could improve the quality and relevance of services provided by humanitarian organisations. However, the sector needs to fully understand the inevitable trade-offs between the services made possible by these data and the potential privacy and security risks for the parties involved. For instance, simply gathering these data or pairing particular data sets can reveal an interest or a relationship that is valuable to third parties.

14 Independent Expert Advisory Group on a Data Revolution for Sustainable Development (IEAG), "A World That Counts – Mobilising the Data Revolution for Sustainable Development," UN Data Revolution (UN Secretary-General, November 2014), http://www.undatarevolution.org/report/.

15 John Warnes, "Using Data to Make Your Humanitarian Organisation More Client-Focused," *UNHCR Innovation Service*, 2017.

So far, however, discussions on legal, political and technological safeguards have been limited. As noted in a recent publication by the ICRC and the Harvard Humanitarian Initiative: "data management comes with enormous legal and ethical responsibilities that most organisations are ill-equipped to handle, both in terms of systems and protocols, but also in terms of institutional culture and attitudes towards privacy."[16]

In the absence of safeguards, service providers are at liberty to give others access to information gathered for humanitarian organisations. The service providers can also add their own datasets to this information. For instance, they can provide another company with a humanitarian organisation's list of cash-transfer recipients and then add their own lists of phone numbers, addresses, or social media accounts.

This information can also be stolen if the provider's security is compromised. Depending on local laws and policies, the information can also be appropriated by private or public authorities. Here, the absence of clear rules on who can access what makes it difficult to defend the "data for good" label. These rules should be straightforward: they should focus on the individual whom the humanitarian organisation is mandated to protect, and they should secure any personal data on which these people's safety might depend.

16 Patrick Vinck, Anne Bennett, and Jacobo Quintanilla, "Engaging with People Affected by Armed Conflicts and Other Situations of Violence – Taking Stock. Mapping Trends. Looking Ahead. Recommendations for Humanitarian Organizations and Donors in the Digital Era" (ICRC, Harvard Humanitarian Initiative, February 2018), https://www.icrc.org/en/publication/engaging-people-affected-armed-conflicts-and-other-siutations-violence.

SECTION 02

Processing data and metadata

Metadata can be approached from three different angles:

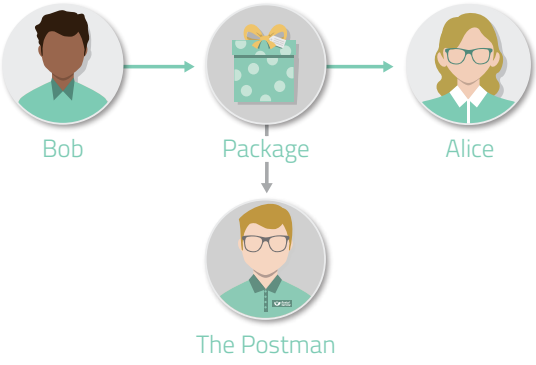
- **From a technical perspective**, the term "metadata" relates primarily to communication protocols. Communication protocols are the practices and standards that determine a message's necessary route: how a letter is sent across the world, or how a phone call, email, or other message is routed across networks. As these different kinds of content move around, metadata are used to ensure that everything gets to the correct destination.
- **From a surveillance perspective**, metadata are data along the communications chain that – in many jurisdictions – enjoy a lesser degree of legal protection than the communication's content. This may be because these jurisdictions have no explicit regulations on accessing and using metadata, or because the regulations they have are intentionally weak. Either way, these data can be accessed and used by various parties for business, legal and surveillance purposes.
- **From a business perspective**, metadata have become a business asset as they provide valuable information on customer behaviour. This information is drawn from the constantly growing number of communications and interactions that people have with modern networks and services.

Different types of data can be identified on the basis of how much control the individual has over their generation and processing.[17]

17 See e.g.: Rochelle Bailis, "Inferred, Declared, Observed... Demystifying Common Data Types," *Hitwise | Competitive Intelligence & Consumer Insights* (blog), January 25, 2016, https://www.hitwise.com/blog/2016/01/inferred-declared-observed-demystifying-common-data-types/; Article 29 Working Party, "Guidelines on the Right to Data Portability" (Directorate General Justice and Consumers | European Commission, April 5, 2017), http://ec.europa.eu/newsroom/document.cfm?doc_id=44099; UK Information Commissioner's Office, "Big Data, Artificial Intelligence, Machine Learning and Data Protection," Data Protection Act and General Data Protection Regulation, September 2017, https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf.

DIAGRAM 02

Different types of data and metadata



The Postman might have an idea of what the package contains based on:

Declared data

Information that is declared on the package, like who is sending it, to whom, and when the package has passed through certain checkpoints.

Inferred data

Information that can be deduced from the declared data or other observations, e.g. the package size, shape or wrapping can give away that it is a gift.

Intent data

Information that can be discerned over time by looking at trends or patterns, e.g. the frequency of packages from Bob to Alice can indicate a relationship.

2.1 Declared data

Definition: **Data knowingly and actively provided by the individual. This can be data that you enter when you set up an account somewhere.**

Declared data can include anything shared during a registration process. For instance, many countries ask individuals to register their identity in order to get a SIM card, open a bank account, or use a social media service. All of this information – names provided, phone or SIM numbers, addresses, biometrics, national identifiers – constitute declared data. Many of these data are generated, gathered, and stored for purposes beyond the technical routing of messages.

- From a **technical** perspective, these data are generated through intentional human actions and are communicated across networks to other service providers
- From a **surveillance** perspective, these data may be solicited pursuant to laws that require personal data to be provided and registered.
- From a **business** perspective, individuals may be required to provide data like their full name and other identification information, or data related to other services used, in order to receive a product or service. "Association" data may also be declared, as individuals identify friends or family. These data might leak from devices to services through poorly designed interfaces, or intentionally through some sort of consent.[18]

18 Here, the notion and framing of consent can be challenging. In March 2018, Facebook was accused of uploading Android users' telephone and messaging metadata to Facebook servers. The company claimed that people had consented to this at some point. However, this claim did not align with the users' own experiences and privacy preferences. For more details see: Privacy International, "Cambridge Analytica and Facebook Are Part of an Industrial Sector That Exploits Your Data," Privacy International, March 20, 2018, http://privacyinternational.org/feature/1681/cambridge-analytica-and-facebook-are-part-industrial-sector-exploits-your-data.

2.2 Inferred and observed data

***Definition*: Data created by service providers and other parties by processing declared data. These data can be created by drawing from declared data leaked from other apps and combining these data with other datasets, and/or applying data analytics to user activities and behaviour.**

Inferred and observed data can include the person's location, drawn from metadata like the last ping from the phone to a cell tower. Friends or close family members can be discerned by observing how frequently an individual interacts with them (e.g. monitoring the number of communications or financial transactions that involve them). In certain cases, these inferences can be more truthful or reliable than declared data.

- From a **technical** perspective, metadata can be used to infer identifying information about the devices an individual uses to connect to or move across different networks.
- From a **surveillance** perspective, metadata can be used to map out people's social networks or relationships. These inferences would also draw on declared data like each member's contact information.
- From a **business** perspective, metadata can be used to monitor people's usage of a particular device and track their movements rather than relying on "check-ins" alone. This can then be used to infer individual characteristics or behavioural patterns.

2.3 Interest and intent data

***Definition*: Data that can only be discerned once large enough amounts of data have been accumulated. These large amounts can then be analysed for trends or patterns, which can be, and often are, used as indicators for intended action.**

Say you always start your day by placing the same order at your local coffee shop. You get there around eight – eight thirty if you've missed your alarm (again). This creates a pattern of financial activity. One day, there is a change: your transaction comes to a different amount, or isn't registered with the same schedule and frequency. This and other observations made from the metadata you generate can reveal new information about you: you've become unemployed, are waking up in a different place, or are saving up for something. However, this information would not have been revealed, nor the inference made, had there not been a long-term behavioural pattern recorded beforehand.

Interest and intent data uses metadata to assign categories or characteristics to people. These can then be monitored. Banks might do this to flag suspicious activity on their client's bank accounts (i.e. activity that does not correspond to the "usual" patterns). If fraudulent activity is confirmed, greater confidence can be assigned to the patterns used to monitor the account.

- From a **technical** perspective, a network might monitor specific forms of behaviour (e.g. a particular signature or key) to protect against or identify attacks.
- From a **surveillance** perspective, inferred or intent data can be used to identify individuals whose activity is deemed suspicious. This activity can be who they call, what they spend their money on, where those payments are made, or their physical movements.
- From a **business** perspective, patterns can be used to identify, monitor and target customer interests with tailored advertisements, content and services. These interests can be considered "confirmed" if the individual engages with the tailored material (e.g. by clicking on the advertisement). The individual's subsequent activities (e.g. searching the web for more information on the advertised product) can be compared to those of other individuals and used to inform intent or future action. Such chains

of reasoning have been used to predict anything from divorce[19] to the behaviour of credit scorers.[20]

The potential value of interest and intent data incentivises service providers to engage in data targeting – the practice of tailoring and showing content that will retain an individual's attention, and entice them to participate in a specific activity (e.g. purchasing a particular product or voting for a particular candidate). In the future, one can imagine this wealth of data being used for automated decision-making and profiling, with implications for how different individuals will be treated in public and private settings. For instance, your online behaviour might affect the services your bank decides to offer you.

This dynamic can create significant risks in conflict or violent settings. In the following sections, this study identifies and discusses a number of potential scenarios for humanitarian organisations.

19 Nicholas Ciarelli, "How Visa Predicts Divorce," *The Daily Beast*, April 6, 2010, Online edition, https://www.thedailybeast.com/how-visa-predicts-divorce.

20 Privacy International, "Fintech: Privacy and Identity in the New Data-Intensive Financial Sector" (Privacy International, November 2017), 28–40, https://privacyinternational.org/sites/default/files/2017-12/Fintech%20report.pdf.

SECTION 03

Threats when processing metadata

3.1 Understanding the legal and policy landscape

Article 12 of the Universal Declaration of Human Rights protects individuals from any arbitrary interference with their "correspondence". This right is upheld by Article 17 of the International Covenant on Political and Civil Rights (ICCPR) and is protected under the constitutions of over 130 countries.[21]

This protection should limit the methods via which government agencies could compel a service provider (e.g. a bank or telephone company) or another third party (e.g. a credit card company or credit bureau) to provide individual records. Under data protection law, the scope of these individual records could, in turn, be limited to the strict minimum amount of data or metadata necessary for the service provider to carry out its work or conduct essential business.

Yet, many global service providers are based in the United States, where no comprehensive data protection law applies to both government and industry. The few protections that do exist do not cover non-US residents – although EU citizens are now protected by the General Data Protection Regulation (GDPR).[22] To date, over 120 countries legally protect personal data held by private and public bodies; around 40 more countries have pending bills or initiatives. The remaining countries – including many in which humanitarian organisations operate – continue to lack any comprehensive data protection framework.[23]

Moreover, existing data protection laws are not always effectively implemented or enforced, nor are they necessarily regularly updated to reflect evolving uses (and abuses) of personal data. This is especially true in places where the rule of law is weak – as humanitarian settings usually

21 See: Privacy International, "What Is Privacy?," Privacy International, http://www.privacyinternational.org/explainer/56/what-privacy.

22 Article 3 (2) of the General Data Protection Regulation (GDPR), which came into force on May 25, 2018, provides that: "This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or b) the monitoring of their behaviour as far as their behaviour takes place within the Union."

23 David Banisar, "National Comprehensive Data Protection/Privacy Laws and Bills 2018," SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, January 25, 2018), https://papers.ssrn.com/abstract=1951416.

are. Such fragile states are unlikely willing or able to effectively pressure global service providers operating on their territory into complying with national data protection laws.

3.1.1 Governments' evolving access to metadata

Globally, governments' access to metadata has increased as a result of their:

- asking for the broader retention of telecommunications and financial metadata;
- mandating the collection of specific data before a good is purchased or a service is provided;
- reducing safeguards on accessing specific and individualised data;
- requiring the advanced monitoring of transactions by service providers in order to detect suspicious activity, tag the relevant individual or account, and report the information to a government body.

In a number of countries, government agencies – including intelligence agencies – have:

- asked for (or assumed) the authority to directly access data held by companies without their involvement or knowledge;
- run their own networks to capture traffic directly or to intercept it from another network;
- gained access to fibre optic cables that carry global telecommunications, including financial sector-related traffic that can then be searched;
- compromised companies' – including financial companies' – telecommunications operations in order to gain direct access without their knowledge;
- established intelligence sharing regimes so that traffic collected by one government is made accessible to another government that may not be able to lawfully collect it itself.

3.1.2 How these surveillance capabilities are exacerbated

1. The rise of transnational companies (i.e. companies with subsidiaries or owners in different countries) means that data can fall under different jurisdictions and therefore be subject to different data protection standards.

2. Metadata can be intercepted by local parties, such as Wi-Fi providers, mobile phone companies, internet service providers, local points of sale, merchants' banks and/or intermediaries.

3. Metadata can be obtained from insecure devices if they are hacked or seized or if an app is programmed to exploit data for commercial purposes (e.g. when an app searches a phone and sends certain data back to the app provider).

4. Insecure services can reveal information if certain data are available for cross referencing (e.g. using information from multiple social feeds to profile someone) or if the service is compromised directly (e.g. through hacking).

5. Service providers may give each other access to certain datasets without the individual's knowledge or consent. For instance, an app provider may be granted access to data held by a social media company.

3.2 Stakeholders in metadata surveillance

Within the scope of this study, stakeholders to be considered include:

1. **People affected by crises.** Individuals affected by conflict, violence or other crises are likely to seek assistance from humanitarian organisations. They might already possess mobile phones with apps, social media accounts, identity documents (some of which might be government-issued), and financial records. In addition, they may have previously provided identifiers including biometrics in order to use a financial or telecommunications service.

2. **Staff and volunteer members of a humanitarian organisation.** This category extends to all individuals in a contractual relationship with a humanitarian organisation, whether local or international. These individuals are likely to have mobile phones. International staff in particular probably have smartphones and use multiple apps, including messaging apps, social media apps, and financial services apps. These may be used for personal and/or professional purposes.

3. **Humanitarian organisations.** This includes organisations with local and international operations. They may run or lease their networks, whose services are accessed by staff, volunteers, and affected people. Although humanitarian organisations have probably signed contracts with telephone networks or financial institutions, they are less likely to have entered into service level contracts with messaging and social media firms (with the exception of conference call or messaging platforms, where corporate contracts are common).

4. **Host government officials.** Depending on the agency (e.g. border, immigration, services), government officials may interact, directly or indirectly, with humanitarian organisations, their staff, volunteers, and affected people. Their services, including IT services, may use domestic providers, including those wholly or partly owned and/or operated by host governments. They might also be outsourced to a global service provider.

5. **Domestic service providers.** These can include Wi-Fi providers, banks, mobile network operators, and internet access providers. They may be local entities or subsidiaries of global providers. The legal framework in which they operate varies from one place to the next.

6. **Domestic companies and other parties to transactions.** This applies to all companies that affected people, staff and volunteers interact with in the conduct of their affairs (e.g. all companies involved in the use of cash transfers to purchase goods and services).

7. **Domestic enforcement agencies.** These agencies may have the legal powers and technical capabilities needed to access and process data (e.g. law enforcement, border, and immigration agencies).

8. **Domestic intelligence agencies.** These agencies may be able to gather data from any of the aforementioned stakeholders. They might also seek data held in other jurisdictions (e.g. a migrant person's country of origin).

9. **Domestic metadata collection unit.** Often mandated by law, this could be a government agency or another entity that collects data for surveillance purposes. In the financial sector, this could be a financial intelligence unit that receives and monitors transactions for suspicious activity. Companies may also play a proactive reporting role (e.g. through Know Your Customer verification services).

10. **Other local or transnational third parties.** These can be any entity that is interested in accessing affected people's data but does not provide affected people with a service (e.g. researchers and non-governmental organisations, but also people traffickers).

11. **Mobile phone operating systems and app stores.** Led by Apple and Google, these organisations design the very rules via which apps interact with device data.

12. **Global service providers.** These are global companies with which affected people or humanitarian organisations knowingly interact (e.g. social media, messaging, or financial providers).

13. **Foreign government agencies.** These agencies interact, directly or indirectly, with humanitarian organisations, their staff and volunteers, and affected people, given the nature of the service they provide (e.g. border and immigration agencies, development agencies, and social services). Their services, including IT services, may use domestic providers – some partly or wholly owned by the government – or they may be outsourced to a global service provider. Under new powers and processes, they may search devices and social media to ascertain the validity of an individual's claims.

14. **Foreign intelligence agencies.** These agencies may directly or indirectly collect data from any of the aforementioned stakeholders, with or without their knowledge/consent.

15. **Transnational communication service providers.** These companies provide services to local and global service providers. In telecommunications, they may include undersea cable and satellite providers or cloud service providers.

16. **Third-party data processing companies in another jurisdiction.** These companies may provide data administering or processing services to any of the stakeholders mentioned above. When doing this, they may collect metadata with or without the original service provider's approval.[24]

24 Examples include third-party scripts run by companies that are able to track usage across the internet; Rapleaf, who would scrape Facebook and other services to gather data on users; and of course the example of Cambridge Analytica is instructive: an app downloaded by some social media users gave access to the data of other people on the same social media service but who had not downloaded the app. See respectively: Jessica Su et al., "De-Anonymizing Web Browsing Data with Social Networks," in *Proceedings of the 26th International Conference on World Wide Web* (Perth, Australia: International World Wide Web Conferences Steering Committee, 2017), 1261–69; Emily Steel and Geoffrey A. Fowler, "Facebook in Privacy Breach," *Wall Street Journal*, October 18, 2010, sec. Tech, http://www.wsj.com/articles/SB10001424052702304772804575558484075236968.

SECTION 04

Where services intersect

This study explores four types of traditional telecommunication services: voice and SMS, messaging applications, cash-transfer programming and social media. While each type of service is discussed separately in the following sections, it is important to note that they may overlap in terms of the entities and operating methods involved.

4.1 Messaging apps and social media

The data processing activities of social media networks and messaging apps must not, and cannot, be viewed as separate. Often, messaging apps are linked to social media networks directly (e.g. Facebook Messenger) or indirectly because they are owned by the same business group (e.g. WhatsApp is owned by Facebook). Here, services may share data for a variety of purposes.

4.1.1 Case study: Facebook and WhatsApp

Facebook acquired WhatsApp in 2014. At the time, WhatsApp's privacy policy prevented the application from sharing any user's personal data with Facebook. Facebook even informed the European Commission that it would be unable to reliably and automatically match Facebook profiles to WhatsApp users.

In August 2016, WhatsApp updated its privacy policy to indicate that WhatsApp would share users' personal data with "the Facebook family of companies" for three purposes: business analysis, system security and targeted advertising. Existing users could withhold consent to the targeted advertising. For any other objection, the only option was to cease using WhatsApp. Here, concerns were raised about the lack of information and options provided to users. In terms of EU data protection requirements, it was alleged that WhatsApp was sharing users' personal data with Facebook without fair notice or a legitimate legal basis.

Before EU data protection legislation was harmonised through the 2018 General Data Protection Regulation (GDPR), various EU member states had ruled that WhatsApp's sharing of personal users' data with Facebook and "the Facebook family of companies" violated existing EU privacy standards. In April 2017, Germany's Higher Administrative Court confirmed an administrative order prohibiting Facebook from

using WhatsApp users' data for its own purposes.[25] In France, formal action was taken against WhatsApp by the Chair of the French data protection authority (CNIL). CNIL claimed that the company had no legal basis to share user data with Facebook and had violated its obligation to cooperate with the French authorities.[26] On 15 March 2018, the Spanish data protection authority (AEDP) released a decision imposing a maximum fine of €300,000 against Facebook and WhatsApp should they process personal data without consent.[27]

Meanwhile, in the UK, a broader investigation was conducted by the Information Commissioner's Office (ICO). The results, presented in May 2018, found that WhatsApp had not identified a lawful basis for the processing and sharing of personal data with Facebook. The company had also failed to provide adequate fair processing information. As such, the sharing of any existing users' information would be incompatible with the purpose for which the data had been obtained and represent a breach of the UK Data Protection Act (1998).[28]

In response to these investigations, WhatsApp publicly committed to not sharing EU users' personal data with Facebook prior to the implementation of the GDPR, on 25 May 2018. Following this date, any data sharing would be done in compliance with the GDPR.[29]

While WhatsApp confirmed, during the investigation, that no EU user's personal data had been shared with Facebook, it is unclear whether the same applies to non-EU users. This would expose a number of individuals, including many in countries affected by conflict or violence, to data targeting in the form of tailored product suggestions, offers or ads.[30]

25 Peter Sayer, "German Court Upholds WhatsApp-Facebook Data Transfer Ban," PCWorld, April 26, 2017, Online edition, sec. News, https://www.pcworld.com/article/3192614/privacy/german-court-upholds-whatsapp-facebook-data-transfer-ban.html.

26 Julia Fioretti, "French Privacy Watchdog Raps WhatsApp over Facebook Data Sharing," *Reuters*, December 18, 2017, Online edition, sec. Technology News, https://www.reuters.com/article/us-whatsapp-privacy-france/whatsapp-faces-french-fine-over-facebook-data-sharing-idUSKBN1EC285.

27 Editorial Board, "La Agencia de Protección de Datos sanciona a Whatsapp y Facebook en España," *El País*, March 15, 2018, sec. Economia, https://elpais.com/economia/2018/03/15/actualidad/1521107973_632714.html.

28 ICO, "ICO Submission to the Inquiry of the House of Lords Select Committee on Communications - The Internet : To Regulate or Not to Regulate?" (London: Information Commissioner's Office, May 16, 2018), https://goo.gl/9tVzHy.

29 "WhatsApp Data Protection Act Undertaking," Data Protection Act 1998 (Information Commissioner's Office; WhatsApp, March 12, 2018), para. 17, https://ico.org.uk/media/action-weve-taken/undertakings/2258376/whatsapp-undertaking-20180312.pdf.

30 See: "WhatsApp Legal Info," WhatsApp.com, April 24, 2018, sec. on affiliated Facebook Companies, https://www.whatsapp.com/legal/#privacy-policy-information-you-and-we-share.

4.2 The financial and telecommunications sector

In certain countries, some telecommunications companies are also active in the financial sector. Examples include mobile operators that provide services like mobile payments.[31] This has interesting implications when it comes to regulatory issues. For example, will users' SIM registration affect the financial services they can receive? Or can someone's access to mobile services be constrained by Know Your Customer regulations?

The financial sector might also attempt to exploit data gathered by messaging and social media alongside the data obtained from their customers in more formal ways. Fintech firms are already exploring how much they can infer about an individual's financial status from the metadata gathered on or generated by their social media activity.[32]

This is discussed in more detail in section 06, on cash-transfer programmes.

31 See: GSMA, "Mobile Network Operator Engagement", https://www.gsma.com/mobilefordevelopment/m4dutilities/mobile-network-operator-engagement/.

32 For more information on the types of new technologies being developed and the role of data within them, see Privacy International's work on fintech, available at: https://privacyinternational.org/topics/fintech.

SECTION 05

Telecommunications and messaging

Broadly speaking, there have been various "generations" of mobile telecommunications:

- **0G: from the 1940s to the 1970s;**
- **1G: from the 1970s to 1980s;**
- **2G: in the 1990s;**
- **3G: in the 2000s;**
- **4G: in the 2010s.**

In the early days of telephones, operators built physical links on switchboards to manually connect cables between the sender and receiver. As the network grew in size, automated switches were configured using in-band signalling protocols – a series of tones at the beginning of the call. However, this mechanism was soon exploited by "Phone Phreaks", who used their own tone generator (dubbed "blue boxes") or even toy whistles (e.g. contained in the American breakfast cereal *Cap'n Crunch*[33]), to place calls free of charge.[34]

This prompted the move, in the late 1970s, to common-channel signalling.[35] This method separated the signalling channel (which would bring up or tear down the required circuits) from the data themselves. Today's public switched telephone network (PSTN, i.e. the sum of all nationally, regionally, or locally operated circuit-switched telephone networks) uses a signalling system called Signalling System No. 7 ("SS7"). SS7 is also the foundation of mobile telephony, used to route calls, SMS, and other mobile services.

In 2008, a series of vulnerabilities in SS7 were unveiled at 25C3,[36] an annual conference among hackers and security experts under the auspices of the Chaos Computer Club.[37] These vulnerabilities allowed cell phone users to be tracked without their knowledge. By 2014, anyone with

33 David Gilmour, "Meet John Draper, the Phone Phreak Who Inspired Apple's Founders," *The Daily Dot*, October 27, 2017, https://www.dailydot.com/layer8/john-draper-captain-crunch/.

34 Ron Rosenbaum, "Secrets of the Little Blue Box," *Esquire Magazine* 76 (1971): 117–25, 222.

35 John G. van Bosse and Fabrizio U. Devetak, *Signaling in Telecommunication Networks* (Wiley, 2006), 111.

36 Tobias Engel, "Locating Mobile Phones Using Signalling System #7," December 27, 2008, https://berlin.ccc.de/~tobias/25c3-locating-mobile-phones.pdf.

37 "Chaos Computer Club (CCC) | Home," ccc.de, https://www.ccc.de/en/?language=en.

the necessary financial resources[38] or technical know-how[39] could exploit SS7 vulnerabilities. In other words, anyone could track a given mobile phone using just the phone number (it was even possible to know how fast a user was travelling along the motorway).

5.1 SMS

The very first SMS message, "Merry Christmas", was sent on the 3 December 1992. SMS messages took advantage of breaks in voice and/or control traffic over SS7 signalling paths. They are entirely unencrypted, openly revealing their sender, receiver, and content. There is also no real guarantee that messages will ever be received, as the transmission is done at a low priority, on a "best effort" basis. Finally, because there is no authentication around SMS messages, it is easy to spoof the identity of the sender.

A number of guidelines have been developed for humanitarian organisations that use SMS to quickly disseminate information in natural disasters or other emergency situations.[40] However, even the use of SMS for humanitarian purposes has also been called into questioned due to several inherent shortfalls:[41]

Cellular networks are not designed to handle crisis-scale traffic loads;

- Targeting users in a specific location is extremely difficult;
- There is no way to authenticate the source of messages;
- SMS is not a real-time service, and message delivery is not always predictable.

38 In 2017, Tech journalist Joseph Cox was offered access to the entire SS7 network for $9,250. See Joseph Cox, "You Can Spy Like the NSA for a Few Thousand Bucks," The *Daily Beast*, November 3, 2017, Online edition, https://www.thedailybeast.com/you-can-spy-like-the-nsa-for-a-few-thousand-bucks.

39 Craig Timberg, "For Sale: Systems That Can Secretly Track Where Cellphone Users Go around the Globe," *Washington Post*, August 24, 2014, Online edition, sec. Technology, https://www.washingtonpost.com/business/technology/for-sale-systems-that-can-secretly-track-where-cellphone-users-go-around-the-globe/2014/08/24/f0700e8a-f003-11e3-bf76-447a5df6411f_story.html.

40 GSMA Disaster Response, "Towards a Code of Conduct: Guidelines for the Use of SMS in Natural Disasters" (GSMA, Souktel, The Qatar Foundation, February 22, 2013), https://www.gsma.com/mobilefordevelopment/programme/mobile-for-humanitarian-innovation/towards-a-code-of-conduct-guidelines-for-the-use-of-sms-in-natural-disasters/.

41 "Report Says That SMS Is Not Ideal for Emergency Communications," *Cellular News*, September 16, 2008, Online edition, http://www.cellular-news.com/story/33684.php; GSMA Disaster Response, "Towards a Code of Conduct."

In his whitepaper on the use of mass SMS in emergency situations,[42] Patrick Traynor (Georgia Institute of Technology) concludes:

> *"Cellular networks are increasingly becoming the primary means of communication during emergencies. Riding the widely-held perception that text messaging is a reliable method of rapidly distributing messages, a large number of colleges, universities and municipalities have spent tens of millions of dollars to deploy third-party EAS over cellular systems. However, this security incident response and recovery mechanism simply does not work as advertised. Through modelling, a series of experiments and corroborating evidence from real-world tests, we have shown that these networks cannot meet the 10 minute alert goal mandated by the public EAS charter and the WARN Act.*
>
> *Moreover, we have demonstrated that the extra text messaging traffic generated by third party EAS will cause congestion in the network and may potentially block upwards of 80% of normal requests, potentially including calls between emergency responders or the public to 9-1-1 services. Accordingly, it is critical that legislators, technologists and the general public understand the fundamental limitations of this mechanism to safeguard physical security and public safety and that future solutions are thoroughly evaluated before they are deployed."*

Indeed, in times of normal operation, there is a message delivery failure rate of 1-5% (often unseen by the end user due to resending schedules). In times of crisis, trying to send mass SMS messages could cause the entire network to saturate and fail. Moreover, cheap access to the internet and internet transport platforms (e.g. 3G or 4G) has led many people to use internet-based messaging apps instead of SMS. Many countries with little physical infrastructure have even become "mobile first" – skipping wired connections entirely and relying instead on 3G or 4G for the provision of mobile broadband.

These 2G, 3G and 4G networks operate at different frequencies, taking advantage of different encryption algorithms between cell phones and towers. While 2G can support encryption, it doesn't necessarily have it switched on by the carrier. Even when encryption is switched on, 2G uses

42 Patrick Traynor, "Characterizing the Security Implications of Third-Party Emergency Alert Systems over Cellular Text Messaging Services," in *Security and Privacy in Communication Networks*, ed. Sushil Jajodia and Jianying Zhou, vol. 50 (Berlin, Heidelberg: Springer Berlin Heidelberg, 2010), 125–43, https://doi.org/10.1007/978-3-642-16161-2_8.

64-bit A5/1 encryption.[43] Inexpensive equipment can be used to crack this encryption in real-time, or retroactively, to access previously collected and stored ciphertext.[44] Breaking 2G encryption can be even easier after a downgrade attack, in which the target phone is forced to use a weaker version of the encryption or none at all.

Whilst the encryption cipher used by 3G for any communications between an endpoint and a cell tower is stronger, it still contains practical weaknesses. Moreover, in order to provide a better data service, the majority of operators use 3G protocols exclusively for data and revert to 2G for voice and SMS. This problem also exists for most 4G implementations, where 4G is used only for data, and voice and SMS are still routed via 2G. The sole exception is Voice over 4G LTE, or VoLTE – but its market penetration remains low and limited mostly to western countries).

Finally, in order to route and move calls from one cell tower to another, there are constant pings of SS7 control messages between a given mobile phone and cell towers in its vicinity. Based on the signal strength between the phone and the towers, the towers "negotiate" between themselves to assign the connection to the "best" tower. This connection changes as the signal strength is continuously monitored, without the call or network being dropped.

However, by constantly monitoring signal strengths, cellular networks continuously track individuals' phones to an approximate location, through triangulation. This isn't necessarily restricted to when the phone is "on" – newer phones ping nearby towers even when they appear to be switched off. Meanwhile, switching phones off for good is becoming less possible given the increasing prevalence of non-removable batteries.

When combined, these rough datasets can provide scores of valuable information. To demonstrate this, a German politician teamed up with Die Zeit in 2012 to turn the data held by his domestic mobile service provider into an interactive map.[45]

43 Alex Biryukov, Adi Shamir, and David Wagner, "Real Time Cryptanalysis of A5/1 on a PC," in *Fast Software Encryption*, Lecture Notes in Computer Science (International Workshop on Fast Software Encryption, Springer, Berlin, Heidelberg, 2000), 1–18, https://doi.org/10.1007/3-540-44706-7_1.

44 Jon Borland, "$15 Phone, 3 Minutes All That's Needed to Eavesdrop on GSM Call," *Ars Technica*, December 29, 2010, Online edition, sec. Tech, https://arstechnica.com/gadgets/2010/12/15-phone-3-minutes-all-thats-needed-to-eavesdrop-on-gsm-call/.

45 Kai Biermann, "Data Protection: Betrayed by our own data," *Zeit*, March 10, 2011, Online edition, sec. Data Protection, https://www.zeit.de/digital/datenschutz/2011-03/data-protection-malte-spitz.

> *"This profile reveals when Spitz walked down the street, when he took a train, when he was in an airplane. It shows where he was in the cities he visited. It shows when he worked and when he slept, when he could be reached by phone and when was unavailable. It shows when he preferred to talk on his phone and when he preferred to send a text message. It shows which beer gardens he liked to visit in his free time. All in all, it reveals an entire life."*

In recent years, however, the rising availability of on-demand data has prompted mobile phone users to move towards messaging apps with end-to-end encryption. These are discussed in the following section.

5.2 Modern messaging protocols

When it comes to communication protocols, there are three main players in the mobile messaging and encryption world: Signal Protocol, MTProto, and iMessage.

- The Signal Protocol (previously known as both Axolotl and TextSecure) is used by OpenWhisper System's Signal, Facebook's WhatsApp, Facebook Messenger (in Secret Conversations[46]). Google Allo (in Incognito Mode[47]), Skype (since mid-2018, in Private Conversations[48]), and Viber (proprietary, modified implementation[49]).
- MTProto was developed and is used by Telegram (in Secret Chats[50]).
- The iMessage protocol was developed by Apple and is used in iMessage.

46 "Messenger Starts Testing End-to-End Encryption with Secret Conversations | Facebook Newsroom," *Facebook Newsroom* (blog), July 8, 2016, https://newsroom.fb.com/news/2016/07/messenger-starts-testing-end-to-end-encryption-with-secret-conversations/.

47 Moxie Marlinspike, "Open Whisper Systems Partners with Google on End-to-End Encryption for Allo," *Signal* (blog), May 18, 2016, https://signal.org/blog/allo/.

48 "What Are Skype Private Conversations?," Skype Support, accessed September 20, 2018, https://support.skype.com/en/faq/FA34824/what-are-skype-private-conversations.

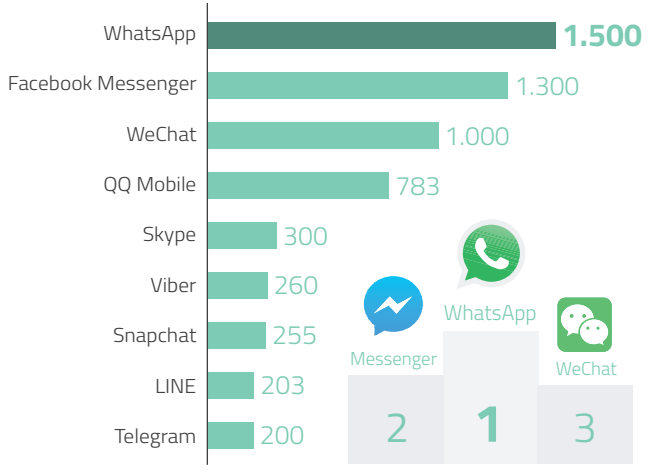
49 "Security," Viber, accessed September 20, 2018, https://www.viber.com/security/.

50 "End-to-End Encryption, Secret Chats," Telegram, accessed September 20, 2018, https://core.telegram.org/api/end-to-end.

DIAGRAM 03

Most popular messaging apps worldwide

Monthly active users in millions



Source: Most popular messaging apps worldwide, as of April 2018, based on number of monthly active users (in millions). Statista, 2018. https://www.statista.com/statistics/258749/most-popular-global-mobile-messenger-apps/

While these messaging protocols all protect message contents to various degrees,[51] there remain issues around the metadata revealed, as well as the platform's privacy, usage, and sharing policies. As stated by Sheryl Sandberg, Chief Operating Officer of Facebook:

> *"The goal for governments is to get as much information as possible. And so when there are message services like WhatsApp that are encrypted, the message itself is encrypted but the metadata [are] not, meaning that you send me a message, we don't know what that message says but we know you contacted me […] If people move off those encrypted services to go to encrypted services in countries that won't share the metadata, the government actually has less information, not more. And so as technology evolves these are complicated conversations, we are in close communication working through the issues all around the world."*[52]

51 Gregorio Zanon, "No, End-to-End Encryption Does Not Prevent Facebook from Accessing WhatsApp Chats," *Medium* (blog), April 12, 2018, https://medium.com/@gzanon/no-end-to-end-encryption-does-not-prevent-facebook-from-accessing-whatsapp-chats-d7c6508731b2.

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

If SMS messages are like postcards (the destination, sender, and message contents can be seen by everyone in the chain), messaging apps are more like closed envelopes. They hide the content of the message, but not the destination or sender. Other information can be inferred from the envelope's characteristics, such as the type of content and message size.

5.2.1 CryptCorp Fictional Case Study

To better illustrate what this might mean for humanitarian organisations, we use the fictional, global service provider CryptCorp. CryptCorp provides an end-to-end encrypted service between Alice and Bob on its "CryptCorp Messenger" (CCM) program. In this scenario, a third person, Eve, is trying to spy on Alice and Bob's communications.

Part 1. SSL/TLS tunnels

To deliver messages, CCM requires a minimum amount of metadata. All of these metadata – i.e. message sender, recipient, time of delivery, and message size – can be seen by Eve.

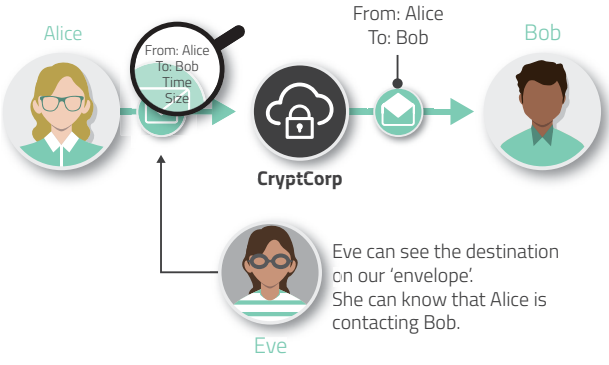
To hide these metadata from Eve, an encrypted "tunnel" (known as SSL or, more accurately, TLS) is used to further encrypt the communications between Alice and Bob through CCM. This would be the equivalent of putting another envelope around the original, and marking CryptCorp as the destination. Now, Eve can only see the message sender, and the global service provider serving as intermediary. This same technology is used to secure communications on bank websites, for example; it is denoted by a green padlock.

Hiding any more metadata from Eve would be nearly impossible without interfering with her ability to access or observe traffic on the network. Once the message has been received by CryptCorp, there is little that Eve can do to get more information without involving CryptCorp (unless Eve is an intelligence agency with significant resources and some form of access to CryptCorp's systems).

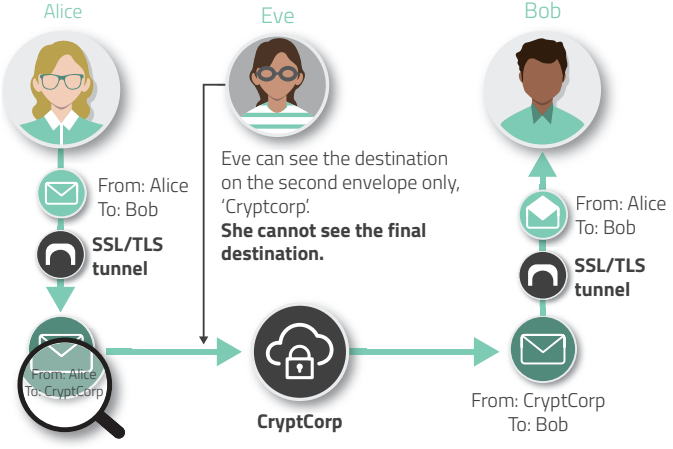
DIAGRAM 04

Obscuring metadata through SSL/TLS tunnels

WITHOUT SSL/TLS TUNNELS



WITH SSL/TLS TUNNELS



Part 2. "Man-in-the-middle" attacks

Eve then decides to call her more tech-savvy colleague Mallory. Mallory knows that there are basically three points of potential failure in Alice's and Bob's communication chain: the tunnel between Alice and CryptCorp; what CryptCorp knows about the message; and the tunnel between CryptCorp and Bob.

Mallory pretends to be CryptCorp and sends Alice all of the information needed to create a tunnel with her. At the same time, Mallory tells CryptCorp that she's Alice, and CryptCorp gives *her* all of the information she needs to create a tunnel with them.

This means that when Alice sends a message to Bob through what she thinks is CryptCorp, she's actually sending it directly to Mallory. Mallory opens the outer envelope, repackages it, and sends it on to CryptCorp for final delivery. This is called a man-in-the-middle attack (MITM). Depending on the sophistication of the man in the middle, this sort of attack can be carried out at an individual, service-provider, or state level.

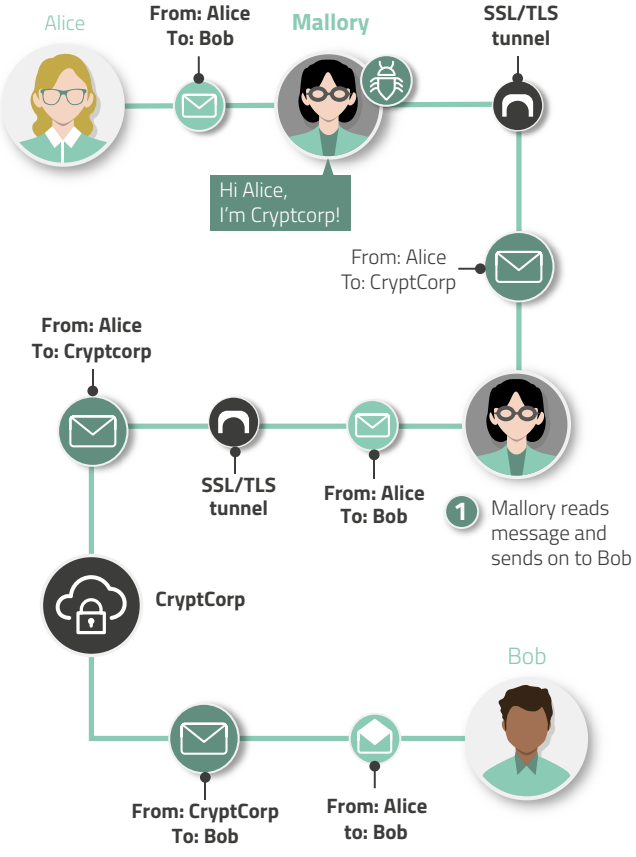
However, these attacks are very unlikely to be successful. Many service providers rely on third-party, independent signatories to authenticate user credentials. If Mallory's credentials are not authenticated by Alice's device (which they shouldn't be, unless Mallory has access to a Certificate Authority and is able to steal or issue fraudulent certificates[53]), Alice will get a warning message. It is worth noting that some states require service providers and citizens to use their own "state certification authorities" instead of, or in addition to, third-party, independent ones. This effectively allows states to act as a mandated man in the middle for all traffic within their borders.[54]

53 See, for example: "Fraudulently Issued Security Certificate Discovered," Factsheet (Dutch Cyber Security & Incident Response Team, September 5, 2011), https://goo.gl/4hkYdk.

54 For examples, see: Nicole Perlroth, "Kazakhstan Moves to Tighten Control of Internet Traffic," *New York Times*, December 3, 2015, sec. Bits Blog, https://bits.blogs.nytimes.com/2015/12/03/kazakhstan-moves-to-tighten-control-of-internet-traffic/; Peter Eckersley, "A Syrian Man-In-The-Middle Attack against Facebook," Electronic Frontier Foundation, May 5, 2011, https://www.eff.org/deeplinks/2011/05/syrian-man-middle-against-facebook; "UAE National PKI Repository," DarkMatter, June 2016, https://ca.darkmatter.ae/UAE/index.html.

DIAGRAM 05

"Man-in-the-middle" attacks



1 **Mallory pretends to be CryptCorp** and sends Alice all of the information needed to create a "tunnel" with her. **At the same time, Mallory tells CryptCorp that she's Alice**, and CryptCorp gives her all of the information she needs to create a "tunnel" with them.

Part 3. Domain fronting

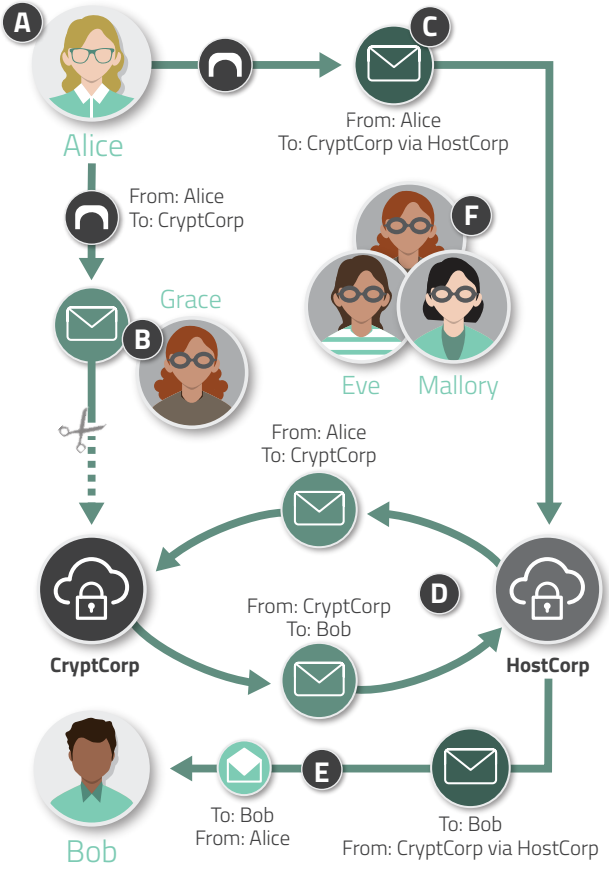
Faced with such prospects, Mallory decides to call her friend Grace. Grace is able to ask all domestic telecommunications service providers to switch off access to CryptCorp. This forces Alice and Bob to revert to less secure communications (e.g. SMS). However, there is a way for programmers at CryptCorp to circumvent this shut-down through something known as "domain fronting".

"Domain fronting" is a technique whereby forbidden hosts (here, CryptCorp) use the domains of permitted hosts (e.g. Google) as a concealing front. In other words, CryptCorp decides to brand all of its communications, on the outside, with the Google domain – or in this scenario, with the domain of the transnational service provider HostCorp. Another domain, which will re-direct to CryptCorp, is encrypted on the inside.

Third parties like the domestic telecommunications providers that Grace alerted cannot distinguish between fronted and non-fronted traffic to a domain. They must choose between allowing all traffic get to a domain – accepting the risk that some of it might be fronted – and blocking all traffic to a domain, which comes at an extremely high cost (e.g. blocking a domain like Google would mean that all Google platforms, services, and websites suddenly lose traffic).

DIAGRAM 06

Domain fronting through HostCorp



A. Alice wants to send a message to Bob via CryptCorp.
B. Grace (at Eve and Mallory's request) shuts down all access to CryptCorp.
C. To continue operating, CryptCorp uses the domain of HostCorp, which is permitted and "too big to be shut down."
D. Now, all CrypCorp communications appear as HostCorp.
E. Alice's message arrives to Bob through CryptCorp posing as HostCorp.
F. Eve, Mallory and Grace cannot distinguish between actual HostCorp activities and CryptCorp-posing-as-HostCorp.

Part 4. State restrictions

One issue that may still arise is the availability of CCM in Alice or Bob's country. Let's say the government banned the use of encrypted services, including encrypted messengers. App stores adhere to this law, meaning that CCM cannot be downloaded from a legitimate source.

Alice and Bob downloaded their version from a web search. However, they cannot know whether this version is a clean copy of the app or has been tampered with (e.g. so as to steal their credentials or even take over their whole phone).[55] Even if the app is clean, neither Alice nor Bob have a way of regularly updating it to newer versions with all of the latest security patches.

5.2.2 Real case studies

In Egypt and the UAE, Signal used domain fronting – with the "fronted domain" being either Google, Amazon CloudFront, or Amazon S3.[56] In Russia, there have been sustained efforts to block Telegram[57] because the application provider refused to surrender user data and encryption keys to the country's security services.[58] Similar efforts were alleged in Iran.[59] In response to domain fronting by Telegram, Russia also blocked nearly 16 million Amazon and Google IP addresses, with huge consequences for unconnected services using Google or Amazon's infrastructure (e.g. ticket sales for museums in the Kremlin, Volvo's aftermarket diagnostics programmes, and Nintendo's online service).[60]

55 Mark Austin, "Did You Download This Fake Ad-Infected WhatsApp from the Google Play Store?," *Digital Trends*, November 5, 2017, Online edition, sec. Social Media, https://www.digitaltrends.com/social-media/fake-whatsapp-google-play-store/; "Fake Whatsapp, Instagram, Facebook on the Google Play Store," Deccan Chronicle, January 31, 2017, https://www.deccanchronicle.com/technology/in-other-news/310117/fake-whatsapp-instagram-facebook-on-the-google-play-store.html.

56 Moxie Marlinspike, "Doodles, Stickers, and Censorship Circumvention for Signal Android," *Signal* (blog), December 21, 2016, https://signal.org/blog/doodles-stickers-censorship/.

57 Maria Kiselyova and Jack Stubbs, "Russia Starts Blocking Telegram Messenger," *Reuters*, April 16, 2018, Online edition, sec. Technology, https://www.reuters.com/article/us-russia-telegram-blocking/russia-starts-blocking-telegram-messenger-regulator-idUSKBN1HN13J.

58 Ilya Khrennikov, "Telegram Loses Bid to Block Russia from Encryption Keys," Bloomberg.Com, March 20, 2018, https://www.bloomberg.com/news/articles/2018-03-20/telegram-loses-bid-to-stop-russia-from-getting-encryption-keys.

59 Heshmat Alavi, "Will Iran Gain Or Lose By Blocking Telegram?," *Forbes*, April 5, 2018, Online edition, https://www.forbes.com/sites/heshmatalavi/2018/04/05/will-iran-gain-or-lose-by-blocking-telegram/.

60 Kimberly Zenz, "Russia Accidentally Sabotages its Internet," *The Daily Beast*, April 19, 2018, Online edition, https://www.thedailybeast.com/russia-accidentally-sabotages-its-internet.

In April 2018, both Google and Amazon stripped their platforms of the functionality required for domain fronting. They both cited, as a motivating factor, the use of domain fronting to obscure malware provenance and hacker activities.[61]

Finally, the protections used in messaging apps have also been compromised by a flaw in SS7. This flaw allows individuals to impersonate a phone number, create a duplicate account on a messaging app, and send and receive all messages destined for this number without the user's knowledge.[62]

61 Abrar Al-Heeti, "Signal Says Amazon, Google Will No Longer Help It Evade Censorship," *CNET*, May 1, 2018, Online edition, sec. Tech Industry, https://www.cnet.com/news/signal-says-amazon-google-will-no-longer-help-it-evade-censorship/; James Sanders, "As Google and AWS Kill Domain Fronting, Users Must Find a New Way to Fight Censorship," *TechRepublic*, May 2, 2018, Online edition, sec. Cyber Security, https://www.techrepublic.com/article/as-google-and-aws-kill-domain-fronting-users-must-find-a-new-way-to-fight-censorship/.

62 vijay, "How To Hack WhatsApp Using SS7 Flaw," *TechWorm* (blog), June 2, 2016, https://www.techworm.net/2016/06/how-to-hack-whatsapp-using-ss7-flaw.html; John Leyden, "SS7 Spookery on the Cheap Allows Hackers to Impersonate Mobile Chat Subscribers," *The Register*, May 10, 2016, Online edition, sec. Security, https://www.theregister.co.uk/2016/05/10/ss7_mobile_chat_hack/.

5.3 Other metadata

Examples of metadata that could be obtained from a message include:

- **IMEI/IMSI (device and SIM identifiers);**
- **sender phone number;**
- **recipient phone number;**
- **message size;**
- **location data;**
- **time data;**
- **IP addresses;**
- **hardware model;**
- **web browser information.**

When aggregated over long periods of time, these metadata can allow various inferences to be made about a person. Joint research by MIT and the Université Catholique de Louvain even found that it only takes four (random) data points to de-anonymise 95% of users:

> *"[T]o extract the complete location information for a single person from an "anonymised" dataset of more than a million people, all you would need to do is place him or her within a couple of hundred yards of a cell-phone transmitter, sometime over the course of an hour, four times in one year. A few Twitter posts would probably provide all the information you needed, if they contained specific information about the person's whereabouts."*[63]

When using a messaging app, it is important to know what is stored by the global messaging service provider, for how long, and why. For example, some messaging apps ask users to regularly provide their contact list, regardless of whether or not these contacts use the platform. Here, information is collected, stored and used for reasons beyond those required to provide the service (e.g. for knowledge of a person's broader usage activity).

Most messaging apps refuse to declare which data they store.[64] In 2017, WhatsApp's parent company, Facebook, issued a transparency report that showed that Facebook had received government requests from 105 out of the 129 countries listed. At least one request had been honoured in 86

63 Larry Hardesty, "How Hard Is It to 'de-Anonymize' Cellphone Data?," MIT News, March 27, 2013, https://news.mit.edu/2013/how-hard-it-de-anonymize-cellphone-data.

64 WhatsApp, OpenWhisper Systems and Telegram were contacted for comment. No responses were received at the time of printing (September 2017).

of those countries.[65] It is not known how many of those requests were for WhatsApp data.

In March 2018, revelations concerning Cambridge Analytica and Facebook also showed that messaging groups were a way to obtain huge amounts of information about users. Let's use WhatsApp as an example. Let's say a humanitarian organisation creates a WhatsApp group to share important information with people located in a conflict area (e.g. where to find water and when the next food distribution will take place). Every member of that group can extract the declared names of other members, their phone numbers, and the messages they sent.[66]

Members of a group conversation can also use the quote feature […] to change the apparent identity of the sender, even if that person is not a member of the group; to alter the text of someone else's reply, essentially putting words in their mouth; and to send a private message disguised as a public message to another group participant. If the targeted individual responds, the reply is visible to everyone in the conversation.[67]

If the group is set up as "public" (i.e. anyone can join without being invited), these data could be accessed by ill-intentioned individuals. For instance, human rights activist Zhang Guanghong was detained after someone reported that he shared an article criticising China's president in a public WhatsApp group.[68] Finally, when a device (e.g. a mobile phone or computer) is seized, forensic tools can be used to access its metadata, including content and data that the user believed to be deleted.

Some access may be restricted through the device's operating system, software, or specific security patches. Newer versions of mobile phone operating systems also include additional security features, like preventing apps from accessing data elsewhere on the device. Users can also choose to grant individual permissions or enable full-device encryption.

65 Facebook, "Facebook Transparency Report", 2017, https://transparency.facebook.com/download/2017-H1/.

66 Vivek Wadhwa, "WhatsApp Public Groups Can Leave User Data Vulnerable to Scraping," *VentureBeat*, April 3, 2018, https://venturebeat-com.cdn.ampproject.org/c/s/venturebeat.com/2018/04/03/whatsapp-public-groups-can-leave-user-data-vulnerable-to-scraping/amp/.

67 Dika Barda, Roman Zaikin, and Oded Vanunu, "FakesApp: A Vulnerability in WhatsApp," Check Point Research, August 7, 2018, https://research.checkpoint.com/fakesapp-a-vulnerability-in-whatsapp/.

68 Paul Mozur, "China Presses its Internet Censorship Efforts across the Globe," *The New York Times*, March 5, 2018, sec. Technology, https://www.nytimes.com/2018/03/02/technology/china-technology-censorship-borders-expansion.html.

Smartphone data used to deport asylum seekers

Recently, several reports have detailed governments' forensic analysis of asylum seekers' smartphones. The data extracted were used to verify claims made in their asylum applications or to obtain new information about their identity, their story, the route they took, etc. Legislation permitting this was adopted in Germany and Denmark in 2017[69] and is now being proposed in Belgium and Austria.[70]

However, these newer devices and operating systems are unlikely to be found in the areas in which humanitarian organisations operate. That means unauthorised third parties may be able to obtain location data, GPS data, contact information in the device or in the apps, and the app data themselves, including transaction metadata.[71]

69 Amar Toor, "Germany Moves to Seize Phone and Laptop Data from People Seeking Asylum," The Verge, March 3, 2017, Online edition, https://www.theverge.com/2017/3/3/14803852/germany-refugee-phone-data-law-privacy.

70 Morgan Meaker, "Europe Is Using Smartphone Data as a Weapon to Deport Refugees," Wired UK, July 2, 2018, https://www.wired.co.uk/article/europe-immigration-refugees-smartphone-metadata-deportations.

71 For reference, see Privacy International's March 2018 report on mobile phone extraction, with a case study on the capabilities of UK police: https://www.privacyinternational.org/campaigns/phone-data-extraction.

5.4 Outsourcing, contracting, and using third parties

Humanitarian organisations usually hire tech companies for two things: one, to develop a tool (e.g. a database or an application); two, to maintain a tool (e.g. a data storage centre).

In both scenarios, the contracting organisation can set specific requirements for the tool's design, including secure data treatment. This is not the case when humanitarian organisations use more popular apps and platforms (e.g. Facebook). In such cases, it is uncommon for the organisation to even sign a contract with the service provider. If a contract was signed, the contract was probably drawn up entirely by the service provider, taking little or no note of the humanitarian organisation's interests or those of the user base it represents.

However, commissioning an *ad hoc* platform or app is not necessarily a valid solution. Let's imagine a humanitarian organisation hires a tech company to develop a new app. A first challenge lies in promoting the app's use among the organisation's beneficiaries. A second challenge is the need to pay for the app's maintenance and security on an ongoing basis. All software, once it has been developed, requires regular updates as new vulnerabilities emerge.

Skype, WhatsApp, and Facebook have all faced security fallacies and failures even though they probably employ some of the brightest minds in the security sector. Even if humanitarian organizations wanted to create their own instruments, they would have to either compete with these companies for such human resources, or use open-source platforms and applications (i.e. platforms and applications whose software is developed in a collaborative manner and then shared openly – like Signal, Drupal, and Tor). By taking this approach, however, humanitarian organisations would be relying on the goodwill of the security sector to identify vulnerabilities.

5.5 Ad networks and tracking

The growth of the web has been almost entirely funded by online advertising. Companies can use their advertisements to track individual behaviour over time and to tailor their message to inferred preferences. While this is why most of the web is free of charge, it also has consequences on privacy.

The systems used to profile users (known as trackers) or their devices (known as fingerprinting) are among the main de-anonymising instruments in existence.[72] By cross-referencing data about specific users and/or devices across different services, advertising networks are able to infer a massive amount of personal information. For instance, 50% of the top 11,000 Android apps on the market use the same 30 advertising networks for in-app advertising. This gives these advertisers huge insights into such things as user behaviour, location data and unique device identifiers.

Since these advertising networks are not built into apps, they access private data through every app that uses a given library rather than through a single app. In other words, if 100 apps installed on your phone use a given library, and you block access for 99 of them, that one remaining app would still be able to give the advertising network all of the data required to track you[73] across everything you do.

On the web, one of the ways that advertising networks track users is through cookies or JavaScript. However, as ad-blocking becomes increasingly prevalent, networks have moved on to new techniques like "device fingerprinting". Say you're using a website with ad-blocking turned on. Information about the device that you're using (including your browser type and version) can still be collected. These properties are used to fingerprint your device.[74] It is then possible to cross-reference fingerprinted devices with users, especially since 80–90% of desktop fingerprints and 81% of mobile device fingerprints have been shown to

72 Fotios Papaodyssefs et al., "Web Identity Translator: Behavioral Advertising and Identity Privacy with Wit," in *Proceedings of the 14th ACM Workshop on Hot Topics in Networks* (ACM, 2015), 1, https://www.recred.eu/sites/default/files/papodyssefs.pdf.

73 Saksham Chitkara, Nishad Gothoskar, Suhas Harish, Jason I. Hong, and Yuvraj Agarwal. 2017. Does this App Really Need My Location? Context-Aware Privacy Management for Smartphones . Proc. ACM Interact. Mob. Wearable Ubiquitous Technol. 1, 3, Article 42 (September 2017), 22 pages. https://doi.org/10.1145/3132029.

74 Steven Englehardt and Arvind Narayanan, "Online Tracking: A 1-Million-Site Measurement and Analysis" (ACM Press, 2016), 2–3, https://doi.org/10.1145/2976749.2978313.

be unique.[75] This form of tracking can reach new scales when numerous websites use the same advertising networks.

These tracking techniques allow advertisements to target ever-more specific subsets of users.[76] Consider, for instance, the famous prank carried out by online marketer Brian Swichkow. Using just a few data points and $1.70, Brian was able to target his roommate with increasingly specific sidebar adverts on Facebook.[77]

Repercussions for the web and the monetisation of user data by social media for funding are discussed in more detail in section 7.

75 Ibid., 3.

76 Paul Vines, Franziska Roesner, and Tadayoshi Kohno, "Exploring ADINT: Using Ad Targeting for Surveillance on a Budget - or - How Alice Can Buy Ads to Track Bob" (ACM Press, 2017), 153–64, https://doi.org/10.1145/3139550.3139567.

77 Brian Swichkow, "How I Pranked My Roommate with Eerily Targeted Facebook Ads," Ghost Influence, September 6, 2014, http://mysocialsherpa.com/the-ultimate-retaliation-pranking-my-roommate-with-targeted-facebook-ads/.

SECTION 06

Cash-transfer programmes (CTP)

"Cash-transfer programmes", "cash-transfer programming", and "cash assistance interventions" refer to providing cash or vouchers directly to people affected by crises.[78] It is a mechanism for delivering assistance, not a programme on its own.[79] The Cash Learning Partnership (CaLP)[80] estimated that USD 2.8 billion were distributed in cash or vouchers in 2016 – that's 40% more than in 2015. Today, approximately 10% of global humanitarian assistance is delivered through CTP.[81]

Proponents of CTP argue that it increases the efficiency, accountability and traceability of aid, while giving affected people more choice and control over their expenses.[82] However, CTP's reliance on technologies and large amounts of metadata can also place affected people at risk.

CTP is used to support the following types of programmes:

- **livelihood protection, recovery, and enhancement,** e.g. funding the purchase of seeds and tools; financing agricultural work; and promoting microeconomic initiatives and small business development;[83]
- **shelter recovery,** e.g. Cash-for-Shelter following the destruction of homes;[84]

78 Kuner and Marelli, *Handbook on Data Protection in Humanitarian Action*, chap. 9.

79 Mercy Corps, "Cash Transfer Programming Toolkit," Toolkit (Mercy Corps, August 26, 2015), 1, https://reliefweb.int/sites/reliefweb.int/files/resources/mercy_corps_cash_transfer_programming_toolkit_part_1.pdf.

80 The CaLP is a global network of humanitarian actors that implement cash-transfer programmes.

81 CaLP, "The State of the World's Cash Report – Cash Transfer Programming in Humanitarian Aid," Executive Summary (CaLP, Accenture, February 2018), http://www.cashlearning.org/downloads/calp-sowc-report-exs-web.pdf.

82 Gabrielle Smith et al., "The State of the World's Cash Report – Cash Transfer Programming in Humanitarian Aid," Full Report (CaLP, Accenture, February 2018), http://www.cashlearning.org/downloads/calp-sowc-report-exs-web.pdf.

83 See e.g.: Cédric Elluard, "Guidance Notes: Cash Transfers in Livelihoods Programming - West Africa," CaLP Learning Workshop (CaLP, February 19, 2016), http://www.cashlearning.org/resources/library/843-guidance-notes-cash-transfers-in-livelihoods-programming--west-africa?keywords=elluard&region=all&country=all&year=all&organisation=all&sector=all&modality=all&language=all&payment_method=all&document_type=all&searched=1.

84 Susie Connolly, "Cash-for-Shelter Pilot Findings in CRS's Typhoon Haiyan Response" (Catholic Relief Services, July 2014), http://www.cashlearning.org/downloads/crs-haiyancash-shelter-pilotmethodology-and-findings2014.pdf.

- **healthcare,** e.g. helping affected people to pay for medical expenses;[85]
- **restoring family links,** e.g. giving cash to help families visit detained relatives;[86]
- **refugee support,** e.g. providing financial assistance to prevent early child marriage in displaced families.[87]

Previously, cash in envelopes was physically distributed to people who had signed up for a CTP. Technological advances have led to new delivery methods, including:

- mobile money, i.e. the use of mobile phones to transfer money;
- bank account transfers;
- smart cards;
- vouchers that can be exchanged for goods or services.[88]

The CTP delivery method is determined by a situation analysis. This analysis usually covers the structure of the economy and local market conditions. For example, to use mobile money, a humanitarian organisation should look at the country's existing mobile money infrastructure as well as the prevalence of mobile phones and what is needed to operate them (e.g. chargers, electricity and an internet connection). The legal context must also be considered.[89]

Finally, various delivery methods can be used simultaneously within a given CTP in order to reach different segments of the population. For example, in Ukraine the ICRC partnered with both the post office and the formal banking sector for its CTP.

85 Ruth Aggiss, "E-Transfers for Hygiene through Red Rose in Northern Syria" (Relief International, September 1, 2016), http://www.cashlearning.org/resources/library/959-e-transfers-for-hygiene-through-red-rose-in-northern-syria?keywords=&region=all&country=all&year=all&organisation=all&sector=wash&modality=all&language=all&payment_method=all&document_type=all&searched=1&pSection=resources&pTitle=library.

86 ICRC, "Guidelines for Cash Transfer Programming" (Geneva: International Red Cross and Red Crescent Movement, 2007), https://www.icrc.org/eng/resources/documents/publication/pguidelines-cash-transfer-programming.htm.

87 Lynn Yoshikawa, "Integrating Cash Transfers into Gender-Based Violence Programs in Jordan: Benefits, Risks and Challenges," Enhanced Response Capacity Project 2014–2015 (International Rescue Committee, February 1, 2016), http://www.cashlearning.org/resources/library/827-integrating-cash-transfers-into-gender-based-violence-programs-in-jordan-benefits-risks-and-challenges-?keywords=&region=all&country=all&year=all&organisation=all&sector=all&modality=all&language=all&payment_method=all&document_type=all&searched=1.

88 ICRC, "Cash Transfer Programming (CTP) - Standard Operating Procedures," ICRC Cash Transfer Programming SOPs (ICRC, January 2018), http://webviz.redcross.org/ctp/docs/en/3.%20resources/1.%20Guidance/1.%20Key%20documents/ICRC%20CTP%20SOPs.pdf.

89 For more on this issue, see: UNCTAD, "Mobile Money for Business Development in the East African Community – A Comparative Study of Existing Platforms and Regulations," ICT Analysis Section (UNCTAD, 2012), sec. D. Regulation and Policy, http://unctad.org/en/PublicationsLibrary/dtlstict2012d2_en.pdf.

6.1 CTP and financial inclusion: benefits and challenges

CTP's digital payment systems can provide "accountable, secure transfers" while promoting the inclusion of segments of the population that might be excluded by traditional cash delivery methods.[90] As more private and public actors deliver this type of service, CTPs can also become more efficient through fair market competition.[91]

Meanwhile, the growing use of digital technology and connectivity is rendering previously "invisible" people "visible" to financial institutions. By creating digital identities and footprints that can be analysed, CTPs are helping many emerging-market consumers' gain access to credit and loans.[92] And when financial institutions partner with humanitarian organisations to identify and reach out to people in need, these digital identities and footprints can help include people who were overlooked under previous programmes.

However, easier access and identification also carry risks. The use of digital technologies for CTP often requires the involvement of numerous, non-humanitarian third parties (e.g. domestic and international mobile network providers, financial institutions and financial intelligence units). This means that humanitarian organisations lose control over the data collected and the metadata generated by the CTP.[93] These data can then be used for non-humanitarian purposes (e.g. to profile potential customers). They can also be shared with external parties out of legal obligation or through partnership agreements.[94]

This latter scenario can pose a serious threat, especially where affected people formerly benefiting from CTP are being targeted by those parties with access to the collected data and metadata. The mere fact that they are seeking assistance from a humanitarian organisation can reveal their affiliation

90 "Doing Cash Differently: How Cash Transfers Can Transform Humanitarian Aid," Report of the High Level Panel on Humanitarian Cash Transfers (Center for Global Development, September 2015), 25, https://www.odi.org/sites/odi.org.uk/files/odi-assets/publications-opinion-files/9828.pdf.

91 Ibid., 25–26.

92 Arjuna Costa, Anamitra Deb, and Michael Kubzansky, "Big Data, Small Credit: The Digital Revolution and Its Impact on Emerging Market Consumers," *Innovations: Technology, Governance, Globalization*, Omidyar Network, 10, no. 3–4 (July 2015): 3–4, https://doi.org/10.1162/inov_a_00240.

93 ICRC, "Cash Transfer Programming (CTP)," sec. 4.

94 Ibid., 31.

with a particular group and expose them to discrimination. In other words, the inevitable visibility created by digital engagement can pose a threat in humanitarian situations.

The individual profiles created through CTPs can also hurt a person's access to credit or loans once the crisis has ended. Imagine a situation in which a financial institution with legal access to the CTP's data labels an individual a "person in a difficult financial situation". Even after the crisis ends, this label might translate into "not creditworthy", hampering that person's access to financial services. As such, digital visibility and profiling can become an instrument for financial discrimination, running counter the original purpose of the CTP.

Of course, many people are already digitally connected to financial services before crises hit. However, this doesn't necessarily mean that they are aware of the risks and vulnerabilities inherent in using these services and how these can play out when there is a sudden change in situation. As such, humanitarian organisations must clearly evaluate and communicate to the people they serve the risks of signing up for a CTP that uses digital technology. These risks are further detailed in the sections below.

6.2 Analysing cash-transfer programming

To safely design a CTP, one must first understand: (1) what data about registered persons are shared with the service provider(s), and (2) what metadata are independently available to the service provider(s) as they carry out their work. This also means understanding the local legal landscape and the requirements applicable to service providers (e.g. an obligation to share data with national authorities and the maximum time limit for data storage).[95]

Humanitarian organisations should also consider the long-term impact of the data generated, directly or indirectly, by CTPs. These data may relate to Know Your Customer requirements[96] applicable to account opening; metadata generated for fund transfers; or data generated when funds or vouchers are used. Considerations should include which, where, by whom, and for how long data are stored at various links in the service provision chain: the mobile network providers, domestic and international financial institutions and banking groups, and domestic and foreign intelligence services. It is worth noting that each of these entities might also be able to share these data with further parties, furthering complicating the situation.

The following sections will examine the issues raised by three different delivery methods used in CTPs. While these focus on the basics, it is worth noting that real cases may involve additional actors and elements.

6.2.1 Mobile money

Mobile phones are often used for CTPs (e.g. to notify people of fund transfers via SMS and to carry out in phone surveys for post-distribution monitoring). However, this section will focus on the use of "mobile money", i.e. the use of mobile phone-based systems for transferring funds.

According GSMA's 2017 *State of the Industry Report on Mobile Money,* mobile money is currently available in 90 countries. While the main area of growth has been sub-Saharan Africa, its use in other parts of the world is

95 See: Kuner and Marelli, *Handbook on Data Protection in Humanitarian Action*, sec. 9.3.1.

96 *Know Your Customer* (KYC) is a process by which businesses check the identity of their customers in order to comply with anti-money laundering and anti-corruption regulations and legislation. See: PwC, "Anti-Money Laundering: Know Your Customer Quick Reference Guide and Global AML Resource Map," PricewaterhouseCoopers, January 2015, https://www.pwc.co.uk/fraud-academy/insights/anti-money-laundering-know-your-customer-quick-ref.html.

also on the rise.[97] Mobile money has been used for CTP in places like Bidi Bidi refugee camp in Uganda,[98] and in Somalia, where almost a third of the USD 44 million sent for the 2016 drought response was delivered through mobile money.[99]

Mobile money works like a basic bank account, with the individual's funds stored in a mobile "wallet". They are able to go to a mobile money agent to deposit or withdraw funds, transfer money to another mobile account, and pay for certain goods and services.

The graph below shows how a CTP is structured using mobile money. While the process may vary from one place to the next, this basic illustration includes the main entities involved in providing the service and the parties with access to the data produced. The specific data each party might have access to, and the potential implications, are further discussed below.

Data held by a domestic service provider

A domestic telecommunications service provider usually has access to:

- unique identifiers for the SIM card and device (IMSI and IMEI numbers);
- time and location of transactions, such as calls and messages;
- billing data;
- data obtained during SIM-card registration.

The data obtained during SIM-card registration may vary considerably from one country to the next and depending on the type of SIM card purchased (e.g. pre-paid vs post-paid). However, there has been a general tendency towards mandatory registration with personally identifiable information, no matter the type of card purchased.[100] This registration often requires a copy of the requestor's ID along with details such as the national identification number and date of birth. It can also involve cross-checking the individual against a national ID database (India

97 GSMA, "State of the Industry Report on Mobile Money," GSMA Mobile Money (GSMA, Bill and Melinda Gates Foundation, Mastercard Foundation, Omidyar Network, 2017), https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2018/02/GSMA_State_Industry_Report_2018_FINAL_WEBv4.pdf.

98 Ibid.

99 Smith et al., "The State of the World's Cash Report," 131–35.

100 Kevin P. Donovan and Aaron K. Martin, "The Rise of African SIM Registration: The Emerging Dynamics of Regulatory Change," *First Monday* 19, no. 2 (January 26, 2014): sec. IV, http://firstmonday.org/ojs/index.php/fm/article/view/4351.

and Pakistan)[101] or taking an individual's fingerprints and photograph (Nigeria).[102]

These requirements are often justified on the basis of preventing or detecting crime. However, research shows that "there are essentially no robust empirical studies that show that such measures make a difference in terms of crime detection as criminals have a number of ways of circumventing rules".[103]

Where SIM registration takes account of on-the-ground realities (such as by not requesting documents that certain segments of the population may not have), it can open up mobile and digital services to people who wouldn't have access to them as unregistered users.[104] As the World Bank observed in its 2016 *ID4Development Strategy*, the pervasiveness of mobile technology provides promising solutions to enrol and authenticate individuals with a unique identification in remote and rural areas.[105] However, if requirements are not aligned with local realities, vulnerable and socially disadvantaged persons may be excluded.[106]

101 GSMA, "Mandatory Registration of Prepaid SIM Cards - Addressing Challenges through Best Practice," GSMA Public Policy (GSMA, April 2016), 33.

102 Ibid.

103 Nicola Jentzsch, "Implications of Mandatory Registration of Mobile Phone Users in Africa," T*elecommunications Policy* 36, no. 8 (September 2012): 612, https://doi.org/10.1016/j.telpol.2012.04.002.

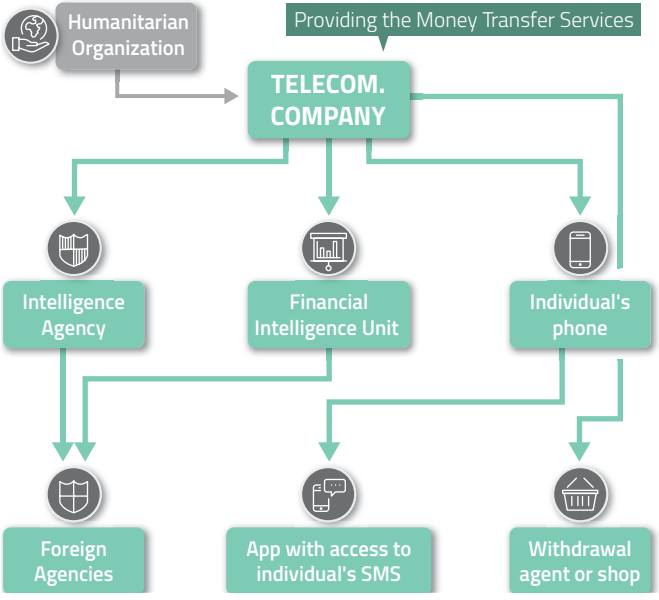
104 GSMA Mobile for Development, "Digital Identity Programme," GSMA, https://www.gsma.com/mobilefordevelopment/digital-identity/.

105 World Bank, "Identification for Development - Strategic Framework," ID4D (World Bank, January 25, 2016).

106 GSMA, "Mandatory Registration of Prepaid SIM Cards - Addressing Challenges through Best Practice."

DIAGRAM 07

How mobile money data can reach other parties



Additional data required for mobile money

Money transfer services often involve the production and storage of additional data and metadata, e.g. through Know Your Customer requirements. These are often far more stringent than identification requirements for SIM registration.

In some cases, these additional requirements have been eased in order to facilitate a CTP. During the 2010 earthquake in Haiti, for example, humanitarian organisations worked with the Haitian government and Central Bank to loosen the Know Your Customer requirements, aligning them with SIM registration data that already included a photo ID and an address.[107]

107 The full Know Your Customer requirements, which were kept for larger transfers, included information such as full name, date and place of birth, type, number, and expiration date of government issued ID, mother's maiden name, address, copy of the government issued ID, and mobile number. See for more information: Avner Levin, Anupa Varghese, and Michelle Chibba, "Know Your Customer Standards and Privacy Recommendations for Cash Transfers," Data Management and Protection, Enhanced Response Capacity Project 2014–2015 (UNHCR, Vision International, April 2015), 14, http://www.cashlearning.org/downloads/erc-know-your-customer-web.pdf.

When conducting mobile money transactions, the domestic telecommunications service provider can store data such as the sender's and recipient's phone numbers, the date and time of the financial transaction, and the transaction ID.[108] Additional information about the transaction is also recorded, such as the location and size of the transaction, the store where it was conducted, and any agents involved at either end.

These data can allow various inferences about a person registered in a CTP, including:

- the fact that they belong to a particular social group, if that group was singled out for humanitarian assistance during that particular period of time;
- where they may have moved after the crisis, using the location records of where they conducted transactions;
- their network of family or friends, based on transfers received or made that didn't involve the humanitarian organisation. Information can then be inferred about these individuals in turn, even though they were not directly involved in the CTP.

The retention period for these data can vary. In Kenya, M-Pesa transaction data are held by the domestic telecommunications service provider Safaricom for "up to seven years or as may be required by any law or regulation".[109] As such, a domestic service provider or any other entity with access to clients' data can draw inferences about these people long after the programme or crisis ends.

Other entities

Various other entities could have access to transaction data from a mobile money transfer. For example, Kenya M-Pesa's terms and conditions state that data and metadata collected as part of their service can be made available to domestic enforcement agencies (e.g. the police), intelligence agencies, financial and public institutions (e.g. the central bank and the anti-corruption commission), domestic metadata collection units, and more.[110] These actors could then infer the same kind of information listed above. This underlines the importance, when selecting a domestic service provider, of understanding who will have access to the data produced by the CTP, and what legal guarantees and obligations they might be subject to.

108 See e.g.: Ignacio Mas and Olga Morawczynski, "Designing Mobile Money Services – Lessons from M-PESA," *Innovations: Technology, Governance, Globalization* 4, no. 2 (2009): 77–91.

109 M-PESA, "M-Pesa Customer Terms & Conditions" (Safaricom's M-PESA Mobile Money Transfer Service, 2018), para. 16.3, https://www.safaricom.co.ke/images/Downloads/Terms_and_Conditions/M-PESA_CUSTOMER_TERS_AND_CONDITIONS.pdf.

110 Ibid., para. 4.

Apps and SMS

Mobile money transaction details are often reported to the recipient via an unencrypted SMS. Going back to the case of M-Pesa in Kenya, these messages quoted the account balance, the date of the transaction, the agent ID, the transaction ID, the transaction type (customer deposit, withdrawal, etc.), the transaction amount, and the recipient's phone number, name, and national ID number.[111] Thus, even when the electronic transfer is encrypted, the details of the transaction are not. Beyond being vulnerable to direct interception (see section 5.1), the information about the transaction remains on the recipients' mobile device.

Yet, access to SMS data is a common request in the initial permissions required by various apps.[112] This means that the app provider can access all transaction details and profile the mobile phone owner. A third party that has access to transaction information could use it to evaluate the creditworthiness of people, potentially undermining their ability to take out loans in the short and long term.[113]

111 Mas and Morawczynski, "Designing Mobile Money Services – Lessons from M-PESA," 85.

112 John Leyden, "Whoah! How Many Google Play Apps Want to Read Your Texts?," *The Register,* July 16, 2014, Online edition, sec. Software, https://www.theregister.co.uk/2014/07/16/google_play_app_permissions_too_lax_argues_permission_control_supplier/.

113 Privacy International, "Fintech: Privacy and Identity in the New Data-Intensive Financial Sector."

Scenario A

Adverse weather is severely damaging the livelihoods of a semi-nomadic group. To prevent the group from engaging in risky financial coping mechanisms, a humanitarian organisation decides to offer cash payments via the local mobile phone operator. Two years later, a regime change suddenly places members of this group at risk of persecution. Domestic law enforcement agencies and intelligence agencies decide to make use of the unrestricted access that financial authorities have to records held by domestic telecommunications service providers. They use these records to identify members of this group, tracking the CTP funds they received two years earlier. The current location of members of this group can also be identified using their phone numbers.

Mitigation: through a prior risk assessment, the humanitarian organisation should have realised that a CTP targeting a specific social group would generate data that could track them over the long term. On that basis, they could have tried to amend the maximum period of data retention, included other groups in the CTP, or opted for a different delivery method.

Scenario B

A person registered in a CTP installs an app that assesses their suitability for a loan. This app generates a credit score based on information provided by the individual, but also information stored on their phone. These data are then sent to the app's data centre.

The company's machine learning algorithm has determined that people registered in a CTP are more likely to be in a vulnerable financial position. In view of the SMS messages indicating this individual's registration in a CTP, the credit score is very low, and the loan is refused.

Mitigation: the humanitarian organisation should systematically anticipate what data will be sent to people registered in CTPs, and in what form. They could then research alternative ways to notify individuals, or at least inform them of the risks involved in SMS communications so that they can act accordingly (e.g. using a feature phone for CTP).

6.2.2 Banking

In some cases, humanitarian organisations use existing banking infrastructure to distribute cash (examples include Mercy Corps in Tajikistan[114] and Oxfam in Iran[115]). This might be done in order to use CTP recipients' existing bank accounts or to help them setup a new one.[116]

Data held by CTP recipient's bank

Most people with a bank account have to comply with the relevant Know Your Customer regulations in the country hosting the account. [117] These regulations vary[118] but often ask for the account holder's name, date of birth, national identification number, and address. Other information can include their tax number and employer details. Often, the domestic financial service provider must see and make copies of all supporting documents (e.g. photo ID). The provider then keeps these copies as long as the account is open.

The bank then records all transactions carried out by its customers. Often, the law requires that banks keep these records for prolonged periods of time. Records include the date, time, location and size of each transaction, the origin of the money received, and where withdrawals were made. Some banks also hold customer's biometrics and/or seek additional information such as whether the customer has social media accounts. Finally, many ATMs have cameras that photograph people making withdrawals. These can be cross-checked with the bank account's owner(s).

Thus, the declared and inferred data that a domestic financial service provider has access to could include:

- periods of informal employment, inferred from irregular payments or spending patterns, for example;
- details of shops where goods are purchased using a debit card (the information might also include the types of goods purchased);
- political views and ideological sympathies, inferred from e.g. regular payments to a political party, subscriptions to periodicals, donations to particular organisations, or diet;

114 Mercy Corps, "Cash Transfer Programming Toolkit," 14.

115 Pantaleo Cretì and Susanne Jaspars, eds., *Cash-Transfer Programming in Emergencies*, Oxfam Skills and Practice (Oxford, UK: Oxfam GB, 2006).

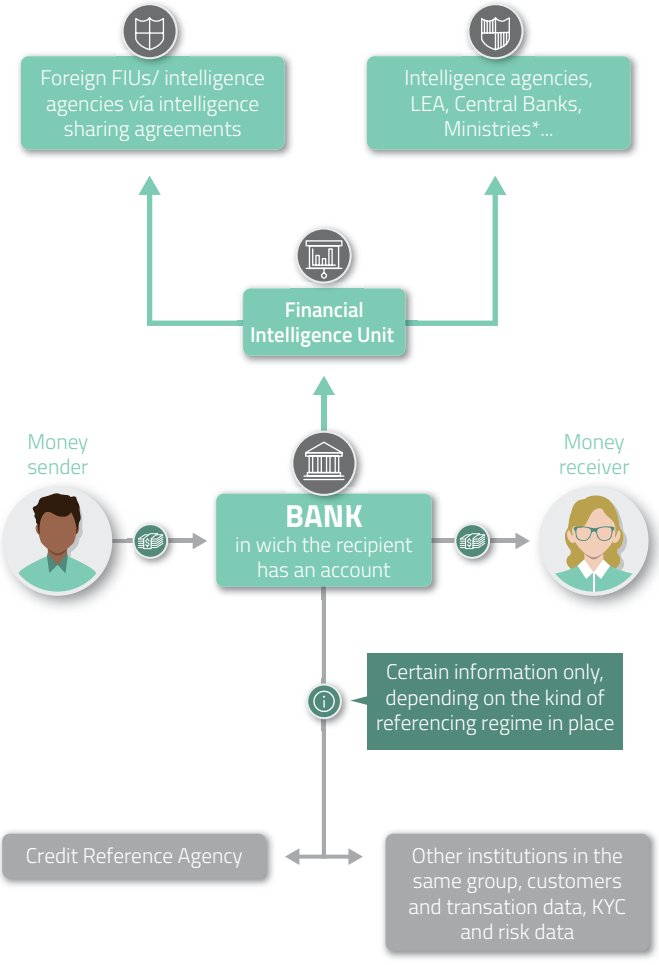
116 Mercy Corps, "Cash Transfer Programming Toolkit," 14.

117 As stated in the previous section, *Know Your Customer* (KYC) is a process enabling businesses to check the identity of their customers in order to comply with money laundering and corruption regulations and legislation. See: PwC, "Anti-Money Laundering."

118 See e.g.: Ibid.

DIAGRAM 08

How banking data can travel to other parties



(*) Depending on the structure of the FIU

- locations where an individual (informally) works and resides, inferred from patterns of spending or locations of ATMs used, for example;
- family and peer networks, and the nature of interactions in those networks;
- religion and the level of devotion over time, inferred from spending around the time of religious festivals or regular payments to religious organisations, for example;
- photographs taken at ATMs;
- periods of financial difficulty or stress.

The provision of humanitarian cash transfers adds to the bank's data records, possibly signalling that the individual or one of his or her peers is in a particular financial situation or position. Given the retention period governing these data under most jurisdictions, this information remains linked to the account for a long period of time.

As such, when selecting a bank to partner with for a CTP, humanitarian organisations must know what information the banks treat as confidential and who has access to any declared or inferred data. It is also important to discuss the data retention period, including once the CTP has ended or the accounts have been closed. This requires a prior understanding of the legal regulations on banking data in that particular country.

Other organisations

Financial services are highly interconnected in a way that humanitarian organisations cannot control. This interconnectedness, as well as national laws, regulations and practices, impacts how data might travel within and outside national borders. This is why humanitarian organisations must discuss, with all institutions involved in the CTP, (1) who their main partners are, nationally and internationally, and (2) whether CTP data can be kept outside any information exchanges.

Financial Intelligence Unit

The Financial Intelligence Unit (FIU) is the national unit whose aim is to fight financial crimes (e.g. money laundering and terrorism funding).[119] FIUs can be part of the judiciary, law enforcement, ministries, or central banks, or a combination of these.[120]

119 "Financial Intelligence Units (FIUs)," The Egmont Group, https://www.egmontgroup.org/en/content/financial-intelligence-units-fius.

120 Ibid.

One of the FIUs' key roles is to analyse the Suspicious Activity Reports (SARs) provided by banks' enforcement units. SARs are designed to detect money laundering and terrorist financing by asking banks to flag transactions they themselves deem "suspicious". The definition of what counts as "suspicious" as well as how this policy is implemented varies.[121] Usually, transactions above a particular amount are flagged automatically, as are transactions involving certain countries or individuals.

Depending on who they might conduct transactions with, people registered in a CTP may have their data sent to an FIU. Once these people's details are shared with the FIU, they are also available to domestic enforcement agencies or domestic intelligence agencies. If the country is part of some international cooperation mechanism to combat money laundering and related crimes, foreign FIUs may also have access to these data, along with their country's government and intelligence agencies.[122]

To anticipate such scenarios, humanitarian organisations should systematically ask FIUs for more information on how transactions come to be labelled as "suspicious" and who gains access to transaction and account holder data once they are labelled "suspicious". This information should also be shared with persons registering in a CTP so they understand what they are consenting to.

Credit Bureaus and similar entities

Credit Bureaus gather or receive information from a wide variety of financial and non-financial entities, including microfinance institutions and credit card companies. They use this information to produce credit scores (i.e. the level of creditworthiness of an individual). [123] The proportion of people covered by a Credit Bureau varies: in OECD high-income countries, 63.7% of adults are covered; in sub-Saharan Africa, only 8.2% of the population is covered.[124] Credit bureau profiles are increasingly used as a primary proof of identity by employers, landlords, and when individuals apply to purchase certain products.

Regulations on which information is available to these agencies vary across territories. However, should this information include data that would label an individual as a CTP recipient (e.g. through previous

121 PwC, "Anti-Money Laundering."

122 See: Egmont Group, "Homepage", https://www.egmontgroup.org/en

123 Not to be confused with credit registries, which are public; credit bureaus are private agencies. See: "Credit Bureau," Key Terms Explained, World Bank, http://www.worldbank.org/en/publication/gfdr/gfdr-2016/background/credit-bureau.

124 "Getting Credit - Doing Business," World Bank Group, June 2017, http://www.doingbusiness.org/data/exploretopics/getting-credit.

transaction data), it could negatively impact their credit score. Not only would this hinders their ability to gain credit, it could also call into question their desirability in the eyes of potential employers, landlords, or sellers of various products.

Other banks and financial institutions

Data held by an individual's domestic financial service provider may be shared with other banks or financial institutions that are members of the same financial group or have the same owner. These institutions may be located in different territories or states, under different jurisdictions. Such data sharing within financial groups is encouraged by the Financial Action Task Force (FATF), an international intergovernmental body.[125] Information shared include transaction data, Know Your Customer details, and other personal data.

Data sharing between financial institutions can place a person registered in a CTP at risk. For example, should this person have fled one country for another, and subsequently opened a new bank account, data sharing between the two institutions may result in the individual's original bank knowing their new location, identity and financial standing. This information could then be accessed by other agencies in the individual's country of origin.

125 FAFT, "Guidance on Private Sector Information Sharing," Guidance Document (Paris: Financial Action Task Force (FATF), 2017), www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-information-sharing.html.

Scenario C

A humanitarian organisation uses a country's existing bank infrastructure for a CTP. Among the persons registered in the programme are people who have fled a neighbouring country. As part of the CTP, recently displaced persons are offered the opportunity to open a bank account in this new country. However, some of these individuals had suffered financial hardship in their country of origin, and had not kept up repayments on loans they had back home. Unbeknownst to them, the new banks in which they open an account are members of the same financial group as their previous bank.

Data-sharing between these entities leads to these individuals' CTP payments being used for loan repayment, leaving them in financial hardship yet again.

Mitigation: the humanitarian organisation should map what data-sharing laws and practices apply in their particular situation. They could then ask that data sharing within the banking group not take place in this instance. This would ensure that no person registered in the CTP is adversely affected and that the CTP actually achieves its objective of financial inclusion.

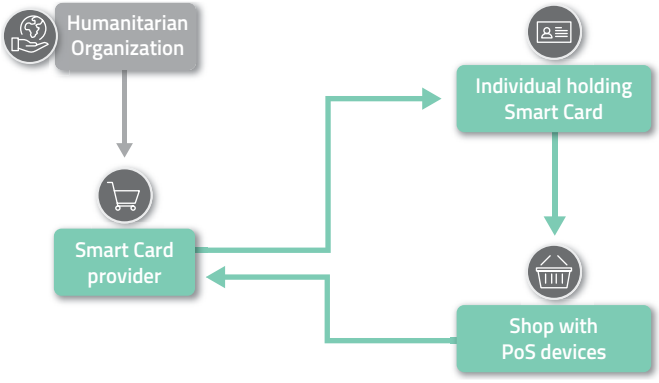
6.2.3 Smartcards

Smartcards are similar to electronic wallets in that they can be used to transfer and spend cash. Their electronic chip links the wallet to a specific owner, and keeps track of their financial balance. Smartcards can be used for cash or for vouchers (which limit their use to particular stores that are part of the initiative). These card-based systems also allow card holdersto access cash or commodities via ATMs or payment merchants, without necessarily having a bank account.[126]

126 Cyprien Fabre and Ruth Aggiss, "Cash-Based Response," ECHO (OECD, 2017), 2, https://www.oecd.org/development/humanitarian-donors/docs/cashbasedresponse.pdf.

DIAGRAM 09

How Smartcards work



Smartcard providers

Smartcards can hold various types of information about their owner, including biometric details.[127] Smartcard systems may involve several providers, including banks,[128] MasterCard,[129] and/or digital transaction providers like sQuid.[130] Shops where the smartcard can be redeemed also require a "Point of Sale" device.

Each Smartcard transaction generates a record which is geo-located and time-stamped and includes the transaction amount and reference information for the device and shop where the transaction was processed.[131] Although the Smartcard provider may not be aware of the card-holder's identity (identifying them only through a unique number), the metadata

127 Valentina Barca et al., "Paying Attention to Detail: How to Transfer Cash in Cash Transfers," *Enterprise Development and Microfinance* 24, no. 1 (March 2013): 10–27, https://doi.org/10.3362/1755-1986.2013.003.

128 Paul Harvey et al., "Delivering Money – Cash Transfer Mechanisms In Emergencies," Cash Learning Partnership (CaLP) (London: CaLP; British Red Cross; Oxfam; Save the Children, 2010), http://www.actionagainsthunger.org/sites/default/files/publications/Delivering_Money-Cash_Transfer_Mechanisms_in_Emergencies_03.2010.pdf.

129 Tobias Flaemig et al., "Using Big Data to Analyse WFP's Digital Cash Programme in Lebanon," *ODI Humanitarian Practice Network* (blog), February 20, 2017, https://odihpn.org/blog/using-big-data-to-analyse-wfps-digital-cash-programme-in-lebanon/.

130 See: "SQuid: Humanitarian Aid & Development," Humanitarian Aid and Development, https://www.squidcard.com/products-solutions/humanitarian-aid-development.

131 Flaemig et al., "Using Big Data to Analyse WFP's Digital Cash Programme in Lebanon."

produced by each transaction could be used to identify the person.[132]

Moreover, data aggregated from Smartcards can give insights into the activities or behavioural patterns of an entire group of people. For example, an analysis of the World Food Programme's Smartcard scheme in Lebanon showed the cardholder's new location and general movements.[133] While seemingly innocuous, these data could be accessible or deliberately shared by private operators of the Smartcard system to actors interested in tracking these groups, or mapping out the particular behavioural patterns of certain members.

Scenario D

A humanitarian organisation offered a CTP to refugees through a Smartcard project. To detect if any fraud had taken place amongst the individuals or shops involved in the programme, the organisation calls upon the Smartcard provider to provide a programme analysis.

The data are anonymised (i.e. all individual names and shop locations are hidden) and shared with an external consultant. Still, the highly-individual nature of transaction data means that individuals could still be de-anonymised and identified. Moreover, the data are very revealing of registered persons' seasonal movements within the country.

Due to national regulations or private agreements, the external consultant's database – dataset included – is accessible to third parties. This means that external groups have access, and may choose to share, refugees' seasonal movements and potential locations. These could be cross-referenced with known locations of social or housing centres. This information could therefore present a serious risk if obtained by groups opposed to hosting refugees.

Mitigation: The humanitarian organisation could have explored measures to minimise the type and amount of data collected to prevent any potential de-anonymisation. Here, it could have sought external advice to design the safest possible system. When outsourcing any kind of analysis or other work, humanitarian organisations should also be wary of where and how the external party will store the information they provide them with, and who might have access to it.

132 Ibid.

133 Ibid.

SECTION 07

Social media platforms

In recent years, the use of social media in times of crisis has grown significantly. Not only can these platforms become lifelines between those seeking assistance and humanitarian organisations, but they also help those affected by crises keep in touch with their loved ones.[134]

7.1

The humanitarian sector's use of social media platforms and data

For humanitarian organisations, physical access to people affected by a crisis isn't always possible or safe. To prevent certain individuals from being isolated from key information cycles, or excluded from any assistance programmes, many organisations are resorting to remote methods of communication.

These are used to provide key information (e.g. where to obtain assistance),[135] gather information (e.g. who needs what and where, or how the situation is evolving),[136] and support programmes.[137]

134 ICRC, "How to Use Social Media to Engage with People Affected by Crisis," News release, *International Committee of the Red Cross* (blog), October 10, 2017, https://www.icrc.org/en/document/social-media-to-engage-with-affected-people.

135 See: ICRC, "Humanitarian Futures for Messaging Apps," Publication, *International Committee of the Red Cross* (blog), January 17, 2017, https://www.icrc.org/en/publication/humanitarian-futures-messaging-apps; Andrea Lunt, "Messaging Apps: The Way Forward for Humanitarian Communication?," ICRC, *Medium* (blog), July 25, 2017, https://medium.com/law-and-policy/messaging-apps-the-way-forward-for-humanitarian-communication-74ab8f3b113e; ICRC, "How to Use Social Media to Engage with People Affected by Crisis."

136 See, for example: Julia Daisy Fraustino, Brooke Liu, and Jan Jin, "Social Media Use during Disasters: A Review of the Knowledge Base and Gaps," Final Report to Human Factors/Behavioral Sciences Division, National Consortium for the Study of Terrorism and Responses to Terrorism (START) (College Park, MD: Science and Technology Directorate, U.S. Department of Homeland Security, December 12, 2012), https://reliefweb.int/report/world/social-media-use-during-disasters-review-knowledge-base-and-gaps; Iffet Turken, "The Power of Social Media When Disaster Strikes," Strategy, *INSEAD Knowledge* (blog), September 21, 2017, https://knowledge.insead.edu/blog/insead-blog/the-power-of-social-media-when-disaster-strikes-7201; Jason Samenow, "Why Social Media Would've Saved Lives during Hurricane Katrina," *Washington Post*, August 28, 2015, Online edition, sec. Capital Weather Gang, https://www.washingtonpost.com/news/capital-weather-gang/wp/2015/08/28/why-social-media-wouldve-saved-lives-during-hurricane-katrina/.

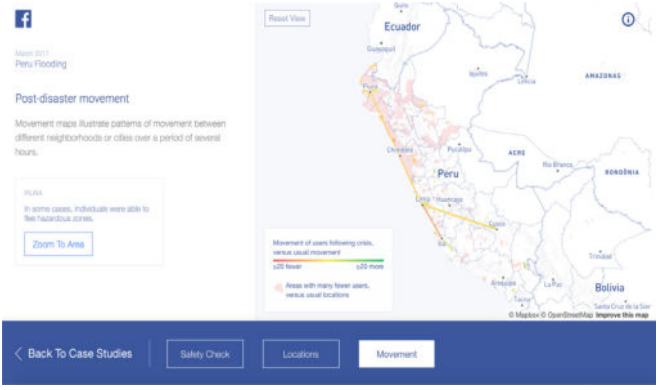
137 See: "Social Media and Forced Displacement: Big Data Analytics & Machine-Learning," White Paper (UNHCR Innovation Service, UN Global Pulse, September 2017), http://www.unhcr.org/innovation/wp-content/uploads/2017/09/FINAL-White-Paper.pdf; ICRC, "How to Use Social Media to Engage with People Affected by Crisis"; "Social Media in Emergencies," *UNHCR | Emergency Handbook* (blog), https://emergency.unhcr.org/entry/168552/social-media-in-emergencies; "Home | United Nations Global Pulse," UN Global Pulse, https://www.unglobalpulse.org/; UNOCHA, "Social Media Monitoring," Guidance, HumanitarianResponse, https://www.humanitarianresponse.info/en/applications/tools/category/social-media-monitoring; "Social Media for Good," *Sm4good* (blog), http://sm4good.com/; UNHCR, "From a Refugee Perspective – Discourse of Arabic Speaking and Afghan Refugees and Migrants on Social Media from March to December 2016," Regional Bureau for Europe – Communicating with Communities Unit (UNHCR, April 2017), http://www.unhcr.org/publications/brochures/5909af4d4/from-a-refugee-perspective.html.

Specifically, advancements in technology and data processing are helping humanitarian organisations to remotely identify, assess and respond to the needs of people affected by crises in the following ways:

- **Information sharing and coordination:** Humanitarian organisations have used social media to better coordinate relief efforts and disseminate information, in real time, to people affected by natural disasters.[138] Indeed, social media "help to integrate and streamline crisis management processes to satisfy the information needs of all stakeholders involved", and "improve the speed and accuracy of crisis communications".[139]
- **Identifying and locating affected people:** Social media data have been used to locate those affected by a particular crisis and understand their movements.[140] Such initiatives help humanitarian organisations to be more effective and targeted in their interventions, as they can identify, locate and map out particular needs over periods of time.

DIAGRAM 10

A demonstration of Facebook's disaster map initiative



Source: Screenshot from Facebook public demo of disaster map initiative. Find out more here – Paige Maas et al., "Facebook Disaster Maps: Methodology," Facebook Research, June 7, 2017, https://research.fb.com/facebook-disaster-maps-methodology.

138 ICRC, "How to Use Social Media to Engage with People Affected by Crisis."

139 Jason Christopher Chan, "The Role of Social Media in Crisis Preparedness, Response and Recovery", Vanguard," Vanguard (RAHS Think Center, 2013).

140 Paige Maas et al., "Facebook Disaster Maps: Methodology," Facebook Research, June 7, 2017, https://research.fb.com/facebook-disaster-maps-methodology.

- **Providing "info-as-aid":** Recent years have seen a growing recognition of "info-as-aid", or the provision of "timely, actionable information as well as safe communications, as forms of aid in their own right".[141] Social media platforms have played a key role in this process as they help share information with crisis-affected persons; they also serve to gather information and feedback from them, in order to better evaluate and adapt humanitarian programmes.[142] In addition, social media data have been used to better identify and target persons for specific information (e.g. taking into account their gender or age).

Mobile map helps residents of Aleppo keep track of water points

In July 2015, a water main broke in Aleppo, northern Syrian. In response, the Syrian Arab Red Crescent, the Aleppo Water Board and the ICRC cleaned 56 drinking water points and set up water tanks across the city. The ICRC's Water and Habitat team in Syria, as well as its Communication team, then posted a map on Facebook and Twitter showing where local residents could find water. The teams also requested feedback to help improve the service. By August, an additional, smartphone-friendly version of the map was published to help people locate their closest water point. Facebook posts related to this mapping project reached ten times as many people as regular posts about ICRC activities in Syria.[143]

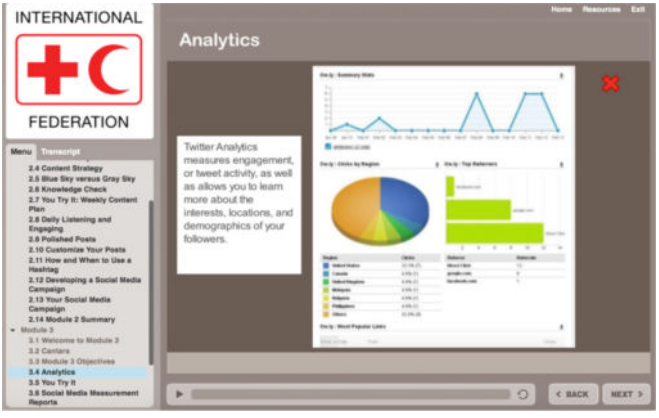
141 Vinck, Bennett, and Quintanilla, "Engaging with People Affected by Armed Conflicts," 11.

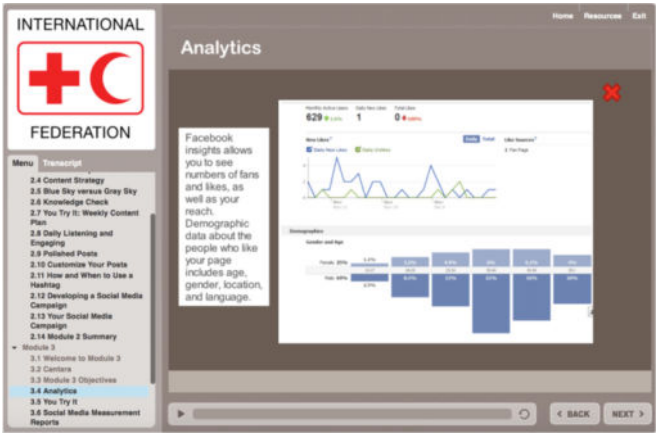
142 Timo Lüge, "How to Use Social Media to Better Engage People Affected by Crises: A Brief Guide for Those Using Social Media in Humanitarian Organizations" (ICRC, IFRC, UNOCHA, September 2017), https://ifrc-1.nyc3.digitaloceanspaces.com/CEASocialmediaguide_WEB_IFRC_EN.pdf.

143 Based on a case study extracted from Ibid.

DIAGRAM 11

Screenshots from the Red Cross and Red Crescent Movement's Social Media E-Learning Course





Source: Screenshot from Module 3 of the "Social Media E-Learning Course: Sharing the Red Cross and Red Crescent Movement on Social Media," Global Disaster Preparedness Center, 2017, https://www.preparecenter.org/ht/node/17141.

- **Understanding perceptions:** Social media can also analyse, in real time, the sentiments of posts by crisis-affected people[144] and "listen" to social media discussions in order to understand their perceptions.[145] This use of social media and analytics has seen increasing interest and exploration by humanitarian organisations looking to better inform their decision-making processes, operational responses and overall policies.[146]

Many promote the use of social media in the development and humanitarian sector as a "tool for good", yet their use can also have negative implications for crisis-affected people, as well as for humanitarian staff and volunteers.[147]

For starters, although organisations' data protection and privacy policies may limit their use of social media, legal and ethical liabilities exist as soon as they involve third-party platforms (e.g. Facebook or Twitter). As discussed in section 5.5, the business model of many of these third-party platforms relies on the exploitation and monetisation of user data.[148] The

144 See: Warnes, "Using Data to Make Your Humanitarian Organisation More Client-Focused"; Matthew L. Williams et al., "Practice Note Using Social Media Data in International Development Research, Monitoring & Evaluation," NatCen Social Research (London: UK Department for International Development, August 2016), fig. 2.1, https://assets.publishing.service.gov.uk/media/57d968c540f0b6533a000052/Social_Media_DFID_Practice_Note_PDF_September_2016_Emily_Poskett.pdf. Figure 2.1, pag. 15,

145 "Analysing Social Media Conversations to Understand Public Perceptions of Sanitation," Global Pulse Project Series (UN Global Pulse, 2014), https://www.unglobalpulse.org/projects/sanitation-social-media; "Informing Governance with Social Media Mining," Pulse Lab Kampala | UNDP, 2016, https://debates.unglobalpulse.net/uganda/.

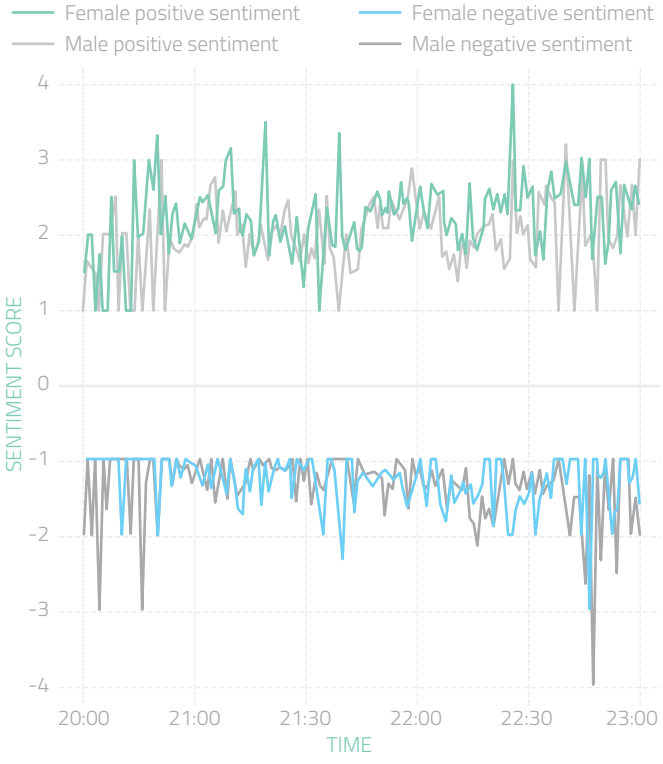
146 Amani Osman, "Social Media E-Learning Course: Sharing the Red Cross and Red Crescent Movement on Social Media," Global Disaster Preparedness Center, 2017, https://www.preparecenter.org/ht/node/17141; "Social Media and Forced Displacement: Big Data Analytics & Machine-Learning"; "Lessons Learned Social Media Monitoring during Humanitarian Crises" (Geneva: ACAPS, September 21, 2015), https://www.acaps.org/sites/acaps/files/resources/files/lessons_learned-social_media_monitoring_during_humanitarian_crises_september_2015.pdf; Christina Newberry, "Social Listening: What It Is, Why You Should Care, and How to Do It Well," Social Media Management, *Hootsuite* (blog), June 13, 2017, https://blog.hootsuite.com/social-listening-business/.

147 Williams et al., "Practice Note Using Social Media Data in International Development Research, Monitoring & Evaluation," fig. 2.1. p. 26.

148 Companies operating in the data exploitation ecosystem generate their profits by selling insights and profiles of their users to interested parties. Most parties focus on commercial advertisements and political campaigning, although some provide financial services. See: Privacy International, "Expose Data Exploitation: Data, Profiling, and Decision Making," Privacy International, https://www.privacyinternational.org/what-we-do/expose-data-exploitation-data-profiling-and-decision-making; Privacy International, "Case Study: Super-Apps and the Exploitative Potential of Mobile Applications," Privacy International, http://www.privacyinternational.org/case-studies/789/case-study-super-apps-and-exploitative-potential-mobile-applications; Privacy International, "Fintech," Privacy International, https://www.privacyinternational.org/topics/fintech; Privacy International, "Case Study: Fintech and the Financial Exploitation of Customer Data," Privacy International, http://www.privacyinternational.org/case-studies/757/case-study-fintech-and-financial-exploitation-customer-data.

DIAGRAM 12

Twitter sentiment towards Ebola outbreak in West Africa in 2014 (over time, by gender)



data collected by these platforms aren't limited to the information actively given by a user; they also include any inferred data stored in what is more commonly known as a "shadow profile".

The inferred data can be any given person's gender, sexuality, religion, location data, interpersonal relationships, and anticipated behaviour (especially if several datasets are correlated, and predictive analytics used). Note that inferred data can be obtained, and deemed more reliable than declared data, even when a user has listed "false" data on

their profile. By engaging with persons over social media, humanitarian organisations are contributing to the generation of the data and metadata upon which these inferences are made.

Refugees' awareness and concern over giving data to social media platforms

Research conducted by Data & Society and the Signal Program on Human Security and Technology at the Harvard Humanitarian Initiative reported that 30% of 135 adult refugees interviewed at the Ritsona camp in Greece expressed concern over giving personal information to social media sites. Another 52% were unconcerned, and 15% were unsure.[149] These figures illustrate the importance for humanitarian organisations to raise awareness of the risks involved with using social media platforms, and in particular with end users.

149 Danielle Poole, Mark Latonero, and Jos Berens, "Refugee Connectivity: A Survey of Mobile Phones, Mental Health, and Privacy at a Syrian Refugee Camp in Greece," Signal Program (Harvard Humanitarian Initiative, Data & Society Research Institute, March 2018), 6, http://hhi.harvard.edu/sites/default/files/publications/refugee_connectivity_web.mb4_.8-2.pdf.

7.2 Social media platforms and data

"Social media" is the collective term used to define websites, applications, and other communication channels dedicated to community-based input, interaction, content-sharing and collaboration. There are an estimated 2.8 billion social media users in the world today; of those, over 90% connect via mobile devices.[150] In 2017, it was reported that 71% of internet users were social media users, with figures expected to increase.[151]

This section discusses the two leading social media platforms used in the humanitarian sector: Facebook and Twitter.[152] Specifically, it explores how these providers operate; what data they generate and process; and how the use of these data by third parties can endanger crisis-affected people and humanitarian staff and jeopardise the neutrality of humanitarian action.

7.2.1 Facebook

With 2.13 billion monthly active users as of 31 December 2017, Facebook has been the leading social media platform for over a decade.[153] According to its company info:

> *"Founded in 2004, Facebook's mission is to give people the power to build community and bring the world closer together. People use Facebook to stay connected with friends and family, to discover what's going on in the world, and to share and express what matters to them."*[154]

Over time, Facebook has continuously expanded the functions of its platform. These include several crisis-specific features, most notably Facebook Crisis Response, which provides users with information during and after natural disasters, terrorist attacks, and other life-threatening

150 Simon Kemp, "Digital in 2017: Global Overview," *We Are Social, Hootsuite* (blog), January 24, 2017, https://wearesocial.com/special-reports/digital-in-2017-global-overview.

151 "Number of Social Media Users Worldwide 2010-2021," Statista, 2018, https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/.

152 This assessment is based on desk-based research of the sector as well as interviews with leading humanitarian organisations.

153 "Social Media – Statistics & Facts," Statista, 2018, https://www.statista.com/topics/1164/social-networks/.

154 "Company Info," *Facebook Newsroom* (blog), 2018, https://newsroom.fb.com/company-info/.

incidents. Through the Safety Check function, it also allows users to mark themselves as "safe" and share this status with their network.

Facebook Crisis Response also provides a space for donations or fund-raising destined to those affected by the situation.[155] Similarly, Facebook's Data for Good division developed and launched Disaster Maps in June 2017. The map draws on users' time-stamped geographic coordinates to show where they are, and where they're headed.[156]

Data

In its Data Policy, Facebook lists the categories of data that it collects when individuals use Facebook services.[157] This includes data declared by the user,[158] but also data provided by others (e.g. content where the individual was tagged) and data about their networks and connections.

155 "Crisis Response," Facebook, https://www.facebook.com/about/crisisresponse/.

156 Maas et al., "Facebook Disaster Maps."

157 "Data Policy," Facebook, April 19, 2018, https://www.facebook.com/policy.php.

158 These usually include name, date of birth, email, gender, religious affiliation, places where the user has lived, education, professional skills, job/work, interests, relationships, as well as all of the content of posts, photos, likes and reactions, and comments.

DIAGRAM 13

Facebook's Data Policy

Things you do and information you provide.

We collect the content and other information that you provide when you use our Services, including when you sign up for an account, create or share, and message or communicate with others. This can include information in or about the content that you provide, such as the location of a photo or the date a file was created. We also collect information about how you use our Services, such as the types of content you view or engage with or the frequency and duration of your activities.

Things others do and information they provide.

We also collect content and information that other people provide when they use our Services, including information about you, such as when they share a photo of you, send a message to you or upload, sync or import your contact information.

Your networks and connections.

We collect information about the people and groups you are connected to and how you interact with them, such as the people you communicate with the most or the groups you like to share with. We also collect contact information that you provide if you upload, sync or import this information (such as an address book) from a device.

Information about payments.

If you use our Services for purchases or financial transactions (e.g. when you buy something on Facebook, make a purchase in a game or make a donation), we collect information about the purchase or transaction. This includes your payment information, such as your credit or debit card number and other card information, and other account and authentication information, as well as billing, shipping and contact details.

Device information.

We collect information from or about the computers, phones or other devices where you install or access our Services, depending on the permissions you've granted. We may associate the information we collect from your different devices, which helps us provide consistent Services across your devices. Examples of the device information that we collect:

- Attributes such as the operating system, hardware version, device settings, file and software names and types, battery and signal strength, and device identifiers.
- Device locations, including specific geographic locations, such as through GPS, Bluetooth or WiFi signals.
- Connection information such as the name of your mobile operator or ISP, browser type, language and time zone, mobile phone number and IP address.

In addition, Facebook automatically collects various metadata, including what the company refers to as "Device data" and "Information about payments". This can mean data extracted from the device being used to access the platform (e.g. its GPS, Bluetooth or Wi-Fi signals, the name of the mobile operator or ISP, the browser type, language used, time zone, mobile phone number, and IP address.) These can then be used to infer information like a specific geographic location and other intelligence.[159]

This information is sometimes shared in the form of data profiles with third-parties looking to target certain users. These profiles are allegedly based on interests, age, location and other information which users provide on their accounts and through their interactions.

Over the years, Facebook has received criticism for shifting its policies from the default assumption of privacy (everything is private unless you choose to share it) to a default assumption of openness (everything is shared unless you choose to make it private).[160] In 2015, it was discovered that users' profiles and network data were shared with third parties every time they used Facebook Login to connect to websites or apps. One of these apps was "This is Your Digital Life", which became the epicentre of the Facebook and Cambridge Analytica controversy in March 2018.

There have also been concerns that new features like Facebook's "Protect" function – although presented as a privacy measure – have actually enabled the company to conduct further data analytics of its users.[161] The "Protect" function was developed by Onavo, a security software company owned by Facebook since 2013. Although Onavo uses a Virtual Private Network (VPN) to securely direct all communications to its servers, it also states that these communications' data will be used to "improve and operate the Onavo service by analysing [the use] of websites, apps and data" and to "improve Facebook products and services, gain insights into the products and services people value, and build better experiences."

159 Larry Kim, "You Won't Believe All the Personal Data Facebook Has Collected on You," *Medium* (blog), December 7, 2016, https://medium.com/the-mission/you-wont-believe-all-the-personal-data-facebook-has-collected-on-you-387c8060ab09; Andreea M. Belu, "The Massive Data Collection by Facebook - Visualized - Dataethical Thinkdotank," *DataEthics* (blog), June 26, 2017, https://dataethics.eu/en/facebooks-data-collection-sharelab/.

160 Agradip Dutta, "Developing an Ethical and Public Policy Approach to Social Media Monitoring during Crises Situation" (School of Public Ethics, Saint Paul University, 2015), 13, https://ruor.uottawa.ca/bitstream/10393/35348/1/Dutta_Agradip_2016_researchpaper.pdf.

161 Michael Potuck, "Facebook's 'Protect' Feature on IOS Essentially Installs Spyware on IPhone and IPad," *9to5Mac* (blog), February 13, 2018, https://9to5mac.com/2018/02/13/facebook-protect-spyware-ios/.

Facebook "Apps"

Facebook also allows users to select "apps" (e.g. games or quizzes) which they can use provided they grant access to their profile. This access results not only in a host of user's own data being shared with the app developer, but also data about their network ("Friends"). This means that even when a user "locks down" their profile, their data could still be collected by a third-party app being used by one of their friends.[162]

On 21 March 2018, following the Cambridge Analytica controversy, Facebook's CEO Mark Zuckerberg promised an app investigation and audit.[163] On 14 May 2018, Facebook announced that "to date, thousands of apps have been investigated and around 200 have been suspended — pending a thorough investigation into whether they did, in fact, misuse any data".[164] The consequences and implications of this investigation for Facebook's data protection and sharing policy have yet to emerge.

7.2.2 Twitter

Twitter is an online news and social networking service where users post and interact in real time with short messages known as "tweets". By the end of 2017, Twitter averaged around 330 million monthly active users.[165]

Data

As per the company's privacy policy, Twitter provides a list of categories of user data that are generated and processed when they use the platform. These include:

- *basic information:* name, username, password, and email address or phone number used to create an account;
- *profile information:* a short biography, location, website, date of birth, and photo;
- *contact information:* email address or phone number;
- *public information:* messages tweeted; metadata generated by each tweet (e.g. time and location); the application used to tweet;

162 "Apps," Facebook Help Center, 2018, https://www.facebook.com/help/1642635852727373/?helpref=hc_fnav.

163 Mark Zuckerberg, "An Update on the Cambridge Analytica Situation," Facebook post, Facebook, March 21, 2018, https://www.facebook.com/zuck/posts/10104712037900071.

164 Ime Archibong, "An Update on Our App Investigation and Audit," Facebook Newsroom (blog), May 14, 2018, https://newsroom.fb.com/news/2018/05/update-on-app-audit/.

165 "Number of Monthly Active Twitter Users Worldwide from 1st Quarter 2010 to 2nd Quarter 2018 (in Millions)," Statista, 2018, https://www.statista.com/statistics/282087/number-of-monthly-active-twitter-users/.

information about the account, such as the date and time it was created, language, country, and time zone; and lists created by the account (e.g. people followed, or tweets liked, retweeted, or otherwise engaged with, e.g. through commenting or "hearting").

Whilst Twitter gives the user the ability to opt out of much of its data processing, its default position is that data shared and published on Twitter are public unless otherwise specified.[166] This means that Twitter is allowed to share or disclose a user's public information (such as profile information, public tweets, or followers) to a wide range of users, services and organisations.[167] Twitter further maintains the right to infer, from these data, which topics might be of interest to the user.[168]

Twitter provides details on how a user can change their default settings to make certain types of data private or inaccessible to Twitter (e.g. by disabling location).[169] The name a user gave to open their account[170] as well as their username, however, remain public unless a user deletes their account. Twitter also processes what its privacy policy calls "Non-Personal, Aggregated, or Device-Level Information". This information includes:

- the total number of times people engaged with a tweet;
- the number of users who clicked on a tweeted link or voted in a tweeted poll;
- the characteristics of a device when it is available to receive an ad;
- topics that people are tweeting about in a particular location;
- aggregated or device-level reports for advertisers about users who saw OR clicked on their ads.

Twitter sometimes shares this information with its business partners,[171] which it splits into two categories:

1. *Real-Time Bidding (RTB) partners:* advertisers can use these partners' systems to buy and serve ads on Twitter.

166 See: "Privacy Policy," Twitter, May 25, 2018, https://twitter.com/content/twitter-com/legal/en/privacy.html.

167 Examples include search engines, developers, and publishers that integrate Twitter content into their services, and organizations such as universities, public health agencies, and market research firms that analyse the information for trends and insights.

168 "Your Twitter Data," Twitter, https://twitter.com/settings/your_twitter_data.

169 "How to Use Precise Location on Mobile Devices," Twitter Help Center, 2018, https://help.twitter.com/en/safety-and-security/twitter-location-services-for-mobile.

170 Twitter does not require users to declare their real name.

171 "Sharing Your Data with Twitter's Business Partners," Twitter, https://help.twitter.com/en/safety-and-security/data-through-partnerships.

2. *Conversion Tracking partners:* partners with whom Twitter shares information for measurement and analytics for advertisers.[172]

The "public" nature of Twitter has resulted in various actors, including humanitarian organisations, using its social media data as an open tool for their own work.[173] While Twitter's "Developer Policies to Protect People's Voices on Twitter" notes that the platform does not allow its search and analytics instruments to be used for surveillance purposes,[174] this has not always prevented misuse by public or private entities (see following section).

DIAGRAM 14

Twitter's RTB and Conversion Tracking Partners (dated 20 Aug 2018)

RTB partners

- Google Doubleclick Bid Manager
- Ubimo
- The Trade Desk
- GroupM UK Limited

Conversion tracking partners

- Adbrix (IGAWorks)
- Adjust
- AdStore Tracking (D.A.Consortium)
- Adways
- AppsFlyer
- Apsalar
- CyberZ
- Doubleclick Campaign Manager
- Kochava
- Singular
- Tune
- Yahoo Japan

172 Ibid.

173 Williams et al., "Practice Note Using Social Media Data in International Development Research, Monitoring & Evaluation," 30.

174 Chris Moody, "Developer Policies to Protect People's Voices on Twitter," *Twitter Developer Blog* (blog), November 22, 2016, https://blog.twitter.com/developer/en_us/topics/community/2016/developer-policies-to-protect-peoples-voices-on-twitter.html.

7.3 Social media metadata

The structure and set-up of social media platforms, as well as the deployment of new functions and services, has led to more and more user data being generated.[175] Some is declared data, i.e. data requested of and provided by a user, for example to register for or benefit from a new service or function.

However, a significant amount of information can be, and is, inferred from these declared data, as well as from the metadata created by the user's interactions and ways of using the service. Here, there is little transparency and accountability regarding how much of this inferred data can be accessed by others; and from which original data they were derived. Moreover, and as stated by Joel Kaplan, Facebook's vice president for U.S. Public Policy, on 8 May 2018:[176]

> "What we've learned over the last couple of years…is that we haven't spent enough time or invested enough in thinking about the ways in which our platform could be abused and the harms that could result from that. There's an element of that that's due to Silicon Valley idealism and optimism. Some of it is due to the fact that we just grew really fast, from Mark's dorm room in 2004 to a service that connected 2 billion people."

7.3.1 Monitoring social media data

Social networks employ a variety of monitoring techniques, generally known as social media monitoring. These techniques rely on different types of data and can be sorted into different groups depending on their sources. The main ones are examined below.

Open source intelligence (OSINT)

Open source intelligence (OSINT) is intelligence gathered from "publicly" available data. This includes articles, news sites, and blog posts, in print and online, clearly intended and available for public use.

175 Dylan Curran, "Are You Ready? This Is All the Data Facebook and Google Have on You | Dylan Curran," *The Guardian*, March 30, 2018, sec. Opinion, http://www.theguardian.com/commentisfree/2018/mar/28/all-the-data-facebook-google-has-on-you-privacy.

176 As quoted in: Michael Igoe, "Facebook Eyes New Partnerships to Better Understand 'High-Risk Areas,'" *Devex*, May 9, 2018, Online edition, sec. Inside Development | Technology, https://www.devex.com/news/sponsored/facebook-eyes-new-partnerships-to-better-understand-high-risk-areas-92721.

Social media intelligence (SOCMINT)

Social Media Intelligence (SOCMINT) can be defined as "the analytical exploitation of information available on social media networks".[177] SOCMINT can often access and make use of both private and public content.

Domestic and foreign enforcement and intelligence agencies have sought more direct access to the data collected by social media platforms and other internet service providers and showed an increased interest in SOCMINT as a "fast, cheap and easy" source of information.[178] Justifications for this increased interest often refer to matters of national security, the fight against terrorism and extremism, tackling cybercrime, and addressing concerns of online hate speech, gender-based violence, and fake news.

SOCMINT can include a governmental agent accessing the site:

- as a non-user (e.g. using a web browser to look through social media content without logging onto the platform);
- as an authenticated user (e.g. @OfficialAgencyHandle following @Suspect);
- using fake profiles (e.g. @JaneDoe following @Suspect);
- by intercepting data streams (e.g. intercepting communications on the user's device or requesting them from the user's internet service provider);
- by requesting data from the social network itself.

Little publicly available information exists on requests made by governments to social media networks, with the exception of what some social media platforms have disclosed in transparency reports.[179] There is also a lack of regulation around covert surveillance techniques, including the use of fake profiles to obtain private or personal information.

177 Evanna Hu, "Responsible Data Concerns with Open Source Intelligence," *Responsible Data* (blog), November 14, 2016, https://responsibledata.io/2016/11/14/responsible-data-open-source-intelligence/.

178 PRISM is a tool used by the US National Security Agency (NSA) to collect private electronic data belonging to users of major internet services like Gmail, Facebook, Outlook, and others. For more details see: Privacy International, "Looking at PRISM - NSA's Mass Surveillance Program," Privacy International, June 7, 2013, http://privacyinternational.org/blog/1363/looking-prism-nsas-mass-surveillance-program; T. C. Sottek and Janus Kopfstein, "Everything You Need to Know about PRISM," *The Verge*, July 17, 2013, Online edition, sec. Policy and Law, https://www.theverge.com/2013/7/17/4517480/nsa-spying-prism-surveillance-cheat-sheet.

179 "Government Requests for User Data," Facebook, 2018, https://transparency.facebook.com/government-data-requests; "Transparency Report," Twitter, 2018, https://transparency.twitter.com/en.html.

Identifying users in a crowd

In the US, the company ZeroFOX came under criticism when a report it had shared with officials of the city of Baltimore was released. In the report, the company showcased how its social media monitoring tool could monitor the riots that followed the funeral of Freddie Gray. Mr Gray was a 25-year-old African American who died while in police custody. The report identified 19 "threat actors", among whom there were two leading figures of the #BlackLivesMatter civil rights movement. Both were qualified as a "physical threat."[180]

Whilst the distinction between "private" and "public" data might have a bearing on the lawfulness of the surveillance, from a technical standpoint, both involve various parties that are neither the user nor the social media provider monitoring social media activities. Concretely, this can mean monitoring the *content* of posts, messages and images or gaining access to membership lists or metadata about photos, tracked locations, etc.

The methods used to analyse data and metadata can vary depending on the social media platforms. Examples include manually reviewing content as it is posted in public or private groups or pages; reviewing the results of user searches and queries; reviewing the activities or types of content posted; and "scraping", which refers to computer programmes systematically extracting content from a web page and replicating it in ways that are directly accessible to the person gathering social media intelligence. Tools can then be applied to the data gathered in order to identify trends and patterns.[181]

180 Stephen Babcock, "ZeroFOX under Fire for Social Media 'Threat Actors' Report during Baltimore Riots - Technical.Ly Baltimore," Technically Baltimore, August 4, 2015, Online edition, sec. Civic, https://technical.ly/baltimore/2015/08/04/zerofox-fire-social-media-threat-actors-report-baltimore-riots/.

181 See Privacy International's explainer on SOCMINT, available at https://www.privacyinternational.org/node/55.

These tools not only analyse data using complex algorithms (e.g. inferring people's political views or potential behaviours from their social media content), but they also organise data into searchable content (e.g. allowing someone to search for people with a *specific* political view or potential behaviour). Often, these processes involve little or no human input.[182]

This kind of intelligence can be used to segment people into categories and target them on these platforms. Numerous studies have shown how individuals can be targeted based on their political opinions or racial characteristics,[183] even when the social media providers attempt or claim to prevent this from happening.[184]

Public vs private data

The "public" nature of social media networks promotes the idea that all data/information that a given social networking site or a given user sets as publicly available can be accessed, collected, and processed with limited regulation, oversight, and safeguards. However, such an interpretation fails to account for the vast collection, retention, use, and sharing of a person's personal data and metadata by both the platform and third parties. It also doesn't consider information that can be inferred from these data, including (but by no means limited to) sensitive personal information such as political affiliation, sexual orientation, or health-care information.

Consider, for instance, a tweet posted from a mobile phone. The user obviously consents, in their privacy settings, to the tweet's content being public. However, they might not consciously consent or indeed realise that they are actually sharing inferred information like their sleeping habits (inferred from patterns of social media presence), their favourite restaurant (inferred from a pattern of tweet locations), or their health status (inferred from a decrease in activity and location patterns corresponding to health-care access points).

182 For further discussion on the concerns regarding the lack of human involvement in automated decision-making, see: Privacy International, "Comments to the Article 29 Working Party Guidelines on Automated Individual Decision-Making and Profiling," Thematic Consultation Submission, Article 29 Working Party Guidelines (Privacy International, November 2017), 29, https://privacyinternational.org/sites/default/files/2017-12/Privacy%20International%20-%20submission%20on%20profiling%20guidance.pdf.

183 Julia Angwin, Madeleine Varner, and Ariana Tobin, "Facebook Enabled Advertisers to Reach 'Jew Haters,'" *ProPublica*, September 14, 2017, sec. Machine Bias, https://www.propublica.org/article/facebook-enabled-advertisers-to-reach-jew-haters.

184 Julia Angwin, "Facebook to Temporarily Block Advertisers From Excluding Audiences by Race," *ProPublica*, November 29, 2017, Online edition, sec. Machine Bias, https://www.propublica.org/article/facebook-to-temporarily-block-advertisers-from-excluding-audiences-by-race.

This is why the question "what are metadata" must be viewed, including by humanitarian organisations, in the context of how the service functions, how privacy and security are addressed in the protocols and the generated data, and what business model is being used.

The European Court of Human Rights: Public vs private

The European Court of Human Rights has long held that "there is [...] a zone of interaction of a person with others, even in a public context, which may fall within the scope of 'private life'".[185] This means that even information or data obtained in a public context can be subject to privacy protection.

As an example, the Court referred to an insurance company's street surveillance of a road accident victim. It stated here that "the normal use of security cameras as such, whether in the street or on public premises, where they serve a legitimate and foreseeable purpose, did not raise an issue under Article 8 of the Convention. However, private-life considerations may arise concerning recording of the data and the systematic or permanent nature of such a record".[186] In other words, using security cameras did not pose a privacy issue *per se* – but systematically recording and storing film from these cameras, especially when they targeted a specific individual, could.

Overall, the court held that a precise legal basis and adequate protection measures were required when surveillance in public spaces interfered with a claimant's personal life, especially when it was being conducted covertly and by public authorities.

7.3.2 Usage of Android apps & permissions

Until recently, Android operating systems had no inbuilt way of allowing users to specify app permissions (e.g. "I want this app to have access to my location, but not my images"). Rather, users had to choose between accepting all requested permissions and not being able to use the app.

185 P.G. and J.H. v. the United Kingdom, Application no. 32792/05, ECHR Judgement, 25 December 2001, para. 56.

186 Vukota-Bojić v. Switzerland, Application no. 61838/10, ECHR Judgement, 18 October 2016, para. 55. The judgement referenced also: Perry v United Kingdom, Merits, Application no. 63737/00, ECHR, 17 July 2003, para. 38-40; and Peck v. the United Kingdom, Application no. 44647/98, ECHR Judgement, 28 January 2003, para. 58-59.

This is problematic for many reasons. Humanitarian organisations operate in areas where people are likely to have older-generation or low-end devices, most of which are probably running outdated versions of Android. If these people are also using social media apps (including at the humanitarian organisation's encouragement), they may be granting that app more access to their device than they realise. For instance, the older Android Facebook app would send all call records, SMS records, and phone contacts to Facebook.

Although limited software support and patching for Android devices exist, it is entirely dependent on the carrier to create and roll these out. In most cases, there are (sometimes significant) time lapses between the identification of a vulnerability and a remedial update (if any) being deployed.

Some community projects try to provide for these updates themselves,[187] including for older devices long abandoned by the manufacturer and carrier. However, using these community releases requires a level of knowledge beyond most casual mobile users. It also carries other risks, such as bricking a phone – rendering it unusable – and rooting – which allows the user to give unrestricted access to apps requesting it

187 LineageOS, "LineageOS Android Distribution," Lineage, https://lineageos.org/.

7.4 Unregulated uses of social media (meta)data

Data and metadata generated, stored, and processed by social media platforms give away much more information about the users than the users usually realise.

Complex analytical methods can be used to infer new information about users on the basis of their declared data, as well as their activities and behaviours on the platform. These inferred data can include social class, occupation, language, ethnicity, religion, sexual orientation, health status, political views, and various consumer preferences. These inferences are derived regardless of the information – whether truthful or not – provided by the user.

Social media monitoring tools: a growing industry

With the growth of the social media industry, a parallel market has emerged for tools that enable and facilitate social media monitoring. These tools, usually called social media monitoring software (SMMS), use complex algorithms to analyse data and organise them in a searchable format.

These types of software are experiencing growing demand as companies, individual politicians, law enforcement, government agencies, defence contractors, and the military try to probe and influence public sentiment based on what is expressed online. This new sector allows them to obtain trend and pattern analyses based on social media data and is gaining attention from actors like data brokers and credit scoring companies.

Beyond monitoring and surveillance, SMMS algorithms can also be used to source trends and evaluate future events and threat assessments.[188]

188 Kimberly McCullough, "Why Government Use of Social Media Monitoring Software Is a Direct Threat to Our Liberty and Privacy," American Civil Liberties Union, May 6, 2016, https://www.aclu.org/blog/privacy-technology/surveillance-technologies/why-government-use-social-media-monitoring.

7.4.1 Financial sector

Previously, financial sector data were limited to what a customer would submit via formal processes. Now, this information is complemented by social media data and metadata.

Loans and social media data

Social media data are being increasingly used to assess the credibility of users requesting loans and to monitor those who have already been given a loan. These assessments are based on a selection of indicators that categorise people as either a "reliable, trustworthy borrower" or an "unreliable, risky borrower".[189] Numerous financial and telecommunications companies such as Tala use various types of social media data, including the number of "friends" and time spent on social media, as part of their assessment processes.

7.4.2 Predicting personal attitudes and traits through data and metadata

It has been demonstrated that (meta)data analysis of a given user or users can help to infer more sensitive personal attitudes and traits. Researchers have used this capacity to analyse political discussions and identify influential political links between users.[190]

In 2013, a study by Cambridge University revealed just how many attributes could be predicted based on a user's Facebook Likes. The algorithm developed was able to infer – as well as or better than people with intimate knowledge of the user – the user's sexual orientation, satisfaction with life, intelligence, emotional stability, religion, alcohol use and drug use, relationship status, age, gender, race, and political views.[191]

Overall: 10 Facebook Likes enabled researchers to know more about a person than a work colleague; and 300 Likes, more than their partner.

189 For more information on the types of new technologies being developed in the financial sector, and the role of data within them, see Privacy International, "Fintech", https://www.privacyinternational.org/topics/fintech.

190 Williams et al., "Practice Note Using Social Media Data in International Development Research, Monitoring & Evaluation."

191 "Digital Records Could Expose Intimates Details and Personality Traits of Millions," University of Cambridge, March 11, 2013, https://www.cam.ac.uk/research/news/digital-records-could-expose-intimate-details-and-personality-traits-of-millions; Michal Kosinski, David Stillwell, and Thore Graepel, "Private Traits and Attributes Are Predictable from Digital Records of Human Behavior," *Proceedings of the National Academy of Sciences*, March 7, 2013, https://doi.org/10.1073/pnas.1218772110.

The research highlighted that "people's personalities could be predicted automatically, without involving human social-cognitive skills.[192] Findings included trends like: "participants with high openness to experience tend to like Salvador Dalí, meditation, or TED talks; participants with high extraversion tend to like partying, Snookie (a "reality show star"), or dancing."[193]

7.4.3 Political campaigning

Although political campaigning has always involved the profiling and targeting of specific broad groups, data can now provide unprecedented levels of detail to inform political messaging at the individual level.[194] An individual may have their location, browsing history, credit score, and social media data cross-referenced to develop a personal profile that can then be used to target them directly with "personalised" messaging.

For instance, in the run-up to the 2017 presidential election in Kenya, Harris Media LCC created the two main political campaigns: *Real Raila* and *Uhuru for Us*. These attacked presidential candidate Raila Odinga.[195] Harris Media used social media data analytics to create political campaigns that targeted audiences based on information inferred from people's social media usage on a range of social media platforms.

In 2018, it was revealed that Cambridge Analytica was collecting user data through a Facebook app called "This Is Your Digital Life". Built by academic Aleksandr Kogan, the app collected not only data from its users (an estimated 270,000), but also from their Facebook friends (amounting to approximately 87 million users). These data were reported to have been used to "build a powerful software program to predict and influence choices at the ballot box."[196]

192 Wu Youyou, Michal Kosinski, and David Stillwell, "Computer-Based Personality Judgments Are More Accurate than Those Made by Humans," *Proceedings of the National Academy of Sciences* 112, no. 4 (January 27, 2015): 1036, https://doi.org/10.1073/pnas.1418680112.

193 Ibid., 1037.

194 Privacy International, "Texas Media Company Hired By Trump Created Kenyan President's Viral 'Anonymous' Attack Campaign Against Rival, New Investigation Reveals," Privacy International, December 15, 2017, http://privacyinternational.org/feature/954/texas-media-company-hired-trump-created-kenyan-presidents-viral-anonymous-attack.

195 Ibid.

196 Carole Cadwalladr and Emma Graham-Harrison, "Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach," *The Guardian*, March 17, 2018, sec. News, https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.. For further information on this issue, see: "The Cambridge Analytica Files", *The Guardian*, https://www.theguardian.com/news/series/cambridge-analytica-files.

This manoeuvre was not identified by Facebook for almost three years.[197] Cambridge Analytica's use of Facebook data illustrates the potential power and insights which may be gained from social media monitoring. This incident raised questions about the lack of regulation on the use of social media data and heightened concerns surrounding the growing collection and monitoring of social media data by third parties and their distribution to other third parties.[198]

7.5 Key considerations: the use of social media by humanitarian organisations

The ways social media platforms are designed, operated and used raise fundamental questions for humanitarian organisations. What happens if the information about members of a Facebook group managed by a humanitarian organisation ends up being used for non-humanitarian purposes, e.g. surveillance? What about if the data of affected individuals are exposed and used for non-humanitarian purposes – can their profiles, their connections, or their location be used to betray or harm them?

What happens if social media data are used to identify, target, and/or undermine the sometimes secret (or at least discreet) operations of a humanitarian organisation in a conflict zone?

As humanitarian organisations use social media to communicate internally or with persons affected by crises, the following factors must be considered:

1. **Humanitarian organisations have no control over the designs and/or safeguards of external services.** When a humanitarian organisation uses a global social media provider to conduct its activities, it is subject to this company's service model and terms and conditions. Unless the organisation is able to negotiate higher and different safeguards, it will incur the same risks as every other user. This includes the risk of data and metadata being centralised and used for non-humanitarian purposes.

197 Yves-Alexandre de Montjoye et al., "Cambridge Analytica Is Only the Beginning and You Might Have Your Friends to Blame for It," *Computational Privacy Group*, March 29, 2018, CPG, Imperial College London edition, https://cpg.doc.ic.ac.uk/blog/cambridge-analytica-is-only-the-beginning/.

198 Privacy International, "Cambridge Analytica and Facebook Are Part of an Industrial Sector That Exploits Your Data."

2. **Increasing amounts of data and metadata are available to third parties.** By using social media, humanitarian organisations are adding to the amount of data collected by service providers and contracted third parties. These data and their uses are beyond the organisation's control, and may be driven by, and used for, non-humanitarian purposes. Even when adjusting privacy settings, users (both the humanitarian organisations and crisis-affected people) have limited control over their data and the information that can be inferred from them.

3. **Humanitarian organisations may be enabling additional targeted monitoring against crisis-affected people.** When engaging with crisis-affected people over social media, humanitarian organisations might request or trigger the generation of personal data or metadata, including location, name and needs. Humanitarian organisations may also use social media and other tools to monitor, listen to or analyse these data to inform their work. However, these very same tools and monitoring mechanisms could also be of great use to traffickers trying to locate vulnerable migrants or States attempting to track political dissidents.

SECTION 08

Conclusion

As humanitarian organisations use newer technologies, they must face up to the associated challenges, risks, and opportunities. This requires greater awareness of the processes and technical implications that these technologies involve. This report has tried to contribute to this awareness, focusing on the existence, impact and potential misuses of data generated, analysed and stored as a result of humanitarian services. In particular, it has addressed a lesser known and highly accessible type of data: metadata, or data about data.

Some metadata are inevitably generated by the use of digital or telecommunication services. In fact, metadata are what allow these services to be delivered. Like an address on a mailed package, metadata convey vital information about who is taking part in a communication, what the overall nature of the communication is, and where that communication is headed.

Together with other types of data collected (declared, inferred, etc.), metadata can lead to a better understanding of people's circumstances and behaviour and inform tailored solutions and more meaningful two-way engagement. However, this capacity to profile, catalogue, and reach individuals also has more troublesome implications, be it with regard to surveillance (by public and private bodies), nudging, targeted advertisements, or discrimination.

Given the humanitarian commitment to "do no harm", it is fundamental that humanitarian practitioners systematically anticipate the risks associated with the use of digital and telecommunication technologies and undertake appropriate measures to mitigate them. Currently, however, many humanitarian organisations lack a clear understanding of what data and metadata are collected and stored by which third-party service providers, and what risks these processes involved. This is partly due to the novelty of this field, as well as to constant changes in the legal, regulatory, and technological landscapes surrounding technologies that generate metadata. However, this evolving landscape is what makes an assessment of the data protection context particularly relevant when humanitarian organisations design their programmes.

In conclusion, two main elements should be kept in mind. First, humanitarian organisations relying on any third parties in their programmes, be they telecommunications or other digital service providers, have little control over the use of the data and metadata produced. Second, data and metadata generated by humanitarian

programmes are more often than not accessible to non-humanitarian third parties with non-humanitarian objectives.

Mapping the life and times of these data is therefore fundamental to ensuring that no harm is done when digital and telecommunication technologies are used. In a nutshell, and as a first step, humanitarian practitioners should always consider mapping:

- what data are required by the service providers they're contracting;
- what metadata are collected by the service provider;
- what metadata are automatically generated as part of the service provision;
- what is declared in the privacy policy of the service provider to which the user consents;
- what do users expressly consent to;
- who has lawful access to these data – beyond the service provider themselves;
- who could have access to these data – e.g. if the service is poorly designed and vulnerable, or if safeguards to prevent access don't exist or are weak;
- how long are these data retained by the service provider, and for what purpose;
- what are the available legal and regulatory safeguards in the relevant territory; and
- can any of the aforementioned elements be negotiated with the service provider.

Meanwhile, additional research should investigate what mitigation options are available for every new digital instrument that makes its way into standard humanitarian operations (e.g. Facebook, WhatsApp, mobile money etc.). Until then, this report can be used as a quick reference to figure out some of the more immediate risks associated with the use of SMS, messaging apps, mobile money, and social media platforms, for example, and to make more informed decisions when determining whether to use them as part of humanitarian programmes.

Glossary

A5/1	Encryption algorithm used in the Global System for Mobile communication (GSM) coding process between an MS (Mobile Station) and the GSM network.
A5/2	Encryption algorithm used in the GSM coding process between an MS (Mobile Station) and the GSM network. This algorithm is simpler than A5/1 and was developed by ETSI (European Telecommunications Standards Institute) for use in Eastern European states with restrictions on certain Western technologies.
De-anonymisation	De-anonymisation is a data-mining strategy whereby anonymous data are cross-referenced with other data sources to re-identify the anonymous data source.
Downgrade attack	A cyber-attack that interferes with the protocol key exchange messages, leading communicating parties to operate with weaker ciphers. Man-in-the-Middle attacks can be an example of downgrade attacks.
HTTP	Hypertext Transport Protocol is a protocol used to carry data on the internet. The protocol supports a variety of data types, media and file formats.
HTTPS	HTTPS (HTTP Secure) is an HTTP extension used to encrypt traffic and protect integrity in communications using SSL/TLS protocols.
IP address	Internet Protocol address (IP address) is a numerical destination address assigned to each device connected to a computer network and using the Internet Protocol for communication.
ISP	An Internet Service Provider is a company that provides internet access to other companies and individuals.
Man In The Middle attack (MITM)	A cyber-attack where a third party places itself between two or more users communicating with each other in order to covertly intercept and possibly alter the communication between them. It is often used to capture credentials, session tokens and other sensitive information that can be used to access a user's system and data. This type of attack is sometimes known as a "Janus attack" or a "bucket brigade attack".

Signalling System No. 7 (SS7)	The signalling system used by today's public switched telephone network, which includes all nationally, regionally, or locally operated circuit-switched telephone networks. SS7 uses common-channel signalling, which means that the signalling channel (the channel that brings up or tears down the circuit needed to route the call or message) is separated from the data of the call or message itself.
Secure Sockets Layer (SSL) **Transport Layer Security (TLS)**	An end-to-end security protocol used to encrypt communications between a client and a server. SSL is being increasingly replaced by more secure encryption algorithms in TLS. The terms SSL and TLS are usually used interchangeably, but in general refer exclusively to TLS.
Web 2.0	Web 2.0 refers to World Wide Web websites that emphasise user-generated content, usability (ease of use, even by non-experts), and interoperability (meaning that a website can work well with other products, systems, and devices) for end users.

Bibliography

Aggiss, Ruth. "E-Transfers for Hygiene through Red Rose in Northern Syria." Relief International, September 1, 2016. http://www.cashlearning.org/resources/library/959-e-transfers-for-hygiene-through-red-rose-in-northern-syria?keywords=&region=all&country=all&year=all&organisation=all&sector=wash&modality=all&language=all&payment_method=all&document_type=all&searched=1&pSection=resources&pTitle=library.

Alavi, Heshmat. "Will Iran Gain Or Lose By Blocking Telegram?" *Forbes*, April 5, 2018, Online edition. https://www.forbes.com/sites/heshmatalavi/2018/04/05/will-iran-gain-or-lose-by-blocking-telegram/.

Al-Heeti, Abrar. "Signal Says Amazon, Google Will No Longer Help It Evade Censorship." *CNET*, May 1, 2018, Online edition, sec. Tech Industry. https://www.cnet.com/news/signal-says-amazon-google-will-no-longer-help-it-evade-censorship/.

"Analysing Social Media Conversations to Understand Public Perceptions of Sanitation." Global Pulse Project Series. UN Global Pulse, 2014. https://www.unglobalpulse.org/projects/sanitation-social-media.

Angwin, Julia. "Facebook to Temporarily Block Advertisers From Excluding Audiences by Race." *ProPublica*, November 29, 2017, Online edition, sec. Machine Bias. https://www.propublica.org/article/facebook-to-temporarily-block-advertisers-from-excluding-audiences-by-race.

Angwin, Julia, Madeleine Varner, and Ariana Tobin. "Facebook Enabled Advertisers to Reach 'Jew Haters.'" *ProPublica*, September 14, 2017, sec. Machine Bias. https://www.propublica.org/article/facebook-enabled-advertisers-to-reach-jew-haters.

"Apps." Facebook Help Center, 2018. https://www.facebook.com/help/1642635852727373/?helpref=hc_fnav.

Archibong, Ime. "An Update on Our App Investigation and Audit." *Facebook Newsroom* (blog), May 14, 2018. https://newsroom.fb.com/news/2018/05/update-on-app-audit/.

Article 29 Working Party. "Guidelines on the Right to Data Portability." Directorate General Justice and Consumers | European Commission, April 5, 2017. http://ec.europa.eu/newsroom/document.cfm?doc_id=44099.

Austin, Mark. "Did You Download This Fake Ad-Infected WhatsApp from the Google Play Store?" *Digital Trends*, November 5, 2017, Online edition, sec. Social Media. https://www.digitaltrends.com/social-media/fake-whatsapp-google-play-store/.

Babcock, Stephen. "ZeroFOX under Fire for Social Media 'Threat Actors' Report during Baltimore Riots - Technical.Ly Baltimore." *Technically Baltimore*, August 4, 2015, Online edition, sec. Civic. https://technical.ly/baltimore/2015/08/04/zerofox-fire-social-media-threat-actors-report-baltimore-riots/.

"BAE Sold Surveillance Tools to Arab States." *BBC News*, June 15, 2017, sec. Middle East. https://www.bbc.com/news/world-middle-east-40276568.

Bailis, Rochelle. "Inferred, Declared, Observed... Demystifying Common Data Types." *Hitwise | Competitive Intelligence & Consumer Insights* (blog), January 25, 2016. https://www.hitwise.com/blog/2016/01/inferred-declared-observed-demystifying-common-data-types/.

Ball, James, and Nick Hopkins. "GCHQ and NSA Targeted Charities, Germans, Israeli PM and EU Chief." *The Guardian*, December 20, 2013, sec. UK news. http://www.theguardian.com/uk-news/2013/dec/20/gchq-targeted-aid-agencies-german-government-eu-commissioner.

Banisar, David. "National Comprehensive Data Protection/Privacy Laws and Bills 2018." SSRN Scholarly Paper. Rochester, NY: Social Science Research Network, January 25, 2018. https://papers.ssrn.com/abstract=1951416.

Barca, Valentina, Alex Hurrell, Ian MacAuslan, Aly Visram, and Jack Willis. "Paying Attention to Detail: How to Transfer Cash in Cash Transfers." *Enterprise Development and Microfinance* 24, no. 1 (March 2013): 10–27. https://doi.org/10.3362/1755-1986.2013.003.

Belu, Andreea M. "The Massive Data Collection by Facebook - Visualized - Dataethical Think-dotank." *DataEthics* (blog), June 26, 2017. https://dataethics.eu/en/facebooks-data-collection-sharelab/.

Biermann, Kai. "Data Protection: Betrayed by our own data." *Zeit*, March 10, 2011, Online edition, sec. Data Protection. https://www.zeit.de/digital/datenschutz/2011-03/data-protection-malte-spitz.

Biryukov, Alex, Adi Shamir, and David Wagner. "Real Time Cryptanalysis of A5/1 on a PC." In *Fast Software Encryption*, 1–18. Lecture Notes in Computer Science. Springer, Berlin, Heidelberg, 2000. https://doi.org/10.1007/3-540-44706-7_1.

Borland, Jon. "$15 Phone, 3 Minutes All That's Needed to Eavesdrop on GSM Call." *Ars Technica*, December 29, 2010, Online edition, sec. Tech. https://arstechnica.com/gadgets/2010/12/15-phone-3-minutes-all-thats-needed-to-eavesdrop-on-gsm-call/.

Bosse, John G. van, and Fabrizio U. Devetak. *Signaling in Telecommunication Networks*. Wiley, 2006.

CaLP. "The State of the World's Cash Report – Cash Transfer Programming in Humanitarian Aid." Executive Summary. CaLP, Accenture, February 2018. http://www.cashlearning.org/downloads/calp-sowc-report-exs-web.pdf.

Chan, Jason Christopher. "The Role of Social Media in Crisis Preparedness, Response and Recovery", Vanguard." Vanguard. RAHS Think Center, 2013.

"Chaos Computer Club (CCC) | Home." ccc.de. https://www.ccc.de/en/?language=en.

Chitkara, Saksham, Nishad Gothoskar, Suhas Harish, Jason I. Hong, and Yuvraj Agarwal. "Does This App Really Need My Location?: Context-Aware Privacy Management for Smartphones." *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 1, no. 3 (September 11, 2017): 1–22. https://doi.org/10.1145/3132029.

Ciarelli, Nicholas. "How Visa Predicts Divorce." *The Daily Beast*, April 6, 2010, Online edition. https://www.thedailybeast.com/how-visa-predicts-divorce.

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

"Company Info." *Facebook Newsroom* (blog), 2018. https://newsroom.fb.com/company-info/.

Connolly, Susie. "Cash-for-Shelter Pilot Findings in CRS's Typhoon Haiyan Response." Catholic Relief

Services, July 2014. http://www.cashlearning.org/downloads/crs-haiyancash-shelter-pilot-methodology-and-findings2014.pdf.

Costa, Arjuna, Anamitra Deb, and Michael Kubzansky. "Big Data, Small Credit: The Digital Revolution and Its Impact on Emerging Market Consumers." *Innovations: Technology, Governance, Globalization*, Omidyar Network, 10, no. 3–4 (July 2015): 49–80. https://doi.org/10.1162/inov_a_00240.

Cox, Joseph. "You Can Spy Like the NSA for a Few Thousand Bucks." *The Daily Beast*, November 3, 2017, Online edition. https://www.thedailybeast.com/you-can-spy-like-the-nsa-for-a-few-thousand-bucks.

"Credit Bureau." Key Terms Explained. World Bank. http://www.worldbank.org/en/publication/gfdr/gfdr-2016/background/credit-bureau.

Cretì, Pantaleo, and Susanne Jaspars, eds. *Cash-Transfer Programming in Emergencies*. Oxfam Skills and Practice. Oxford, UK: Oxfam GB, 2006.

"Crisis Response." Facebook. https://www.facebook.com/about/crisisresponse/.

Curran, Dylan. "Are You Ready? This Is All the Data Facebook and Google Have on You | Dylan Curran." *The Guardian*, March 30, 2018, sec. Opinion. http://www.theguardian.com/commentisfree/2018/mar/28/all-the-data-facebook-google-has-on-you-privacy.

"Data Policy." Facebook, April 19, 2018. https://www.facebook.com/policy.php.

Daynes, Leigh. "Doctors of the World: How We Discovered GCHQ Was Spying on Us." *OpenDemocracy*, April 20, 2015, Online edition. https://www.opendemocracy.net/digitaliberties/leigh-daynes/doctors-of-world-how-we-discovered-gchq-was-spying-on-our-operations.

"Digital Records Could Expose Intimate Details and Personality Traits of Millions." University of Cambridge, March 11, 2013. https://www.cam.ac.uk/research/news/digital-records-could-expose-intimate-details-and-personality-traits-of-millions.

"Doing Cash Differently: How Cash Transfers Can Transform Humanitarian Aid." Report of the High Level Panel on Humanitarian Cash Transfers. Center for Global Development, September 2015. https://www.odi.org/sites/odi.org.uk/files/odi-assets/publications-opinion-files/9828.pdf.

Donovan, Kevin P., and Aaron K. Martin. "The Rise of African SIM Registration: The Emerging Dynamics of Regulatory Change." *First Monday* 19, no. 2 (January 26, 2014). http://firstmonday.org/ojs/index.php/fm/article/view/4351.

Dutta, Agradip. "Developing an Ethical and Public Policy Approach to Social Media Monitoring during Crises Situation." Major research paper submitted to the Faculty of Human Sciences and Philosophy, School of Public Ethics, Saint Paul University, 2015. https://ruor.uottawa.ca/bitstream/10393/35348/1/Dutta_Agradip_2016_researchpaper.pdf.

Eckersley, Peter. "A Syrian Man-In-The-Middle Attack against Facebook." Electronic Frontier Foundation, May 5, 2011. https://www.eff.org/deeplinks/2011/05/syrian-man-middle-against-facebook.

Editorial Board. "La Agencia de Protección de Datos sanciona a Whatsapp y Facebook en España." *El*

País. March 15, 2018, sec. Economia. https://elpais.com/economia/2018/03/15/actualidad/1521107973_632714.html.

Elluard, Cédric. "Guidance Notes: Cash Transfers in Livelihoods Programming- West Africa." CaLP Learning Workshop. CaLP, February 19, 2016. http://www.cashlearning.org/resources/library/843-guidance-notes-cash-transfers-in-livelihoods-programming--west-africa?keywords=elluard&region=all&country=all&year=all&organisation=all&sector=all&modality=all&language=all&payment_method=all&document_type=all&searched=1.

"End-to-End Encryption, Secret Chats." Telegram. https://core.telegram.org/api/end-to-end.

Engel, Tobias. "Locating Mobile Phones Using Signalling System #7." PowerPoint presented at the 25th Chaos Computer Club Congress, December 27, 2008. https://berlin.ccc.de/~tobias/25c3-locating-mobile-phones.pdf.

Englehardt, Steven, and Arvind Narayanan. "Online Tracking: A 1-Million-Site Measurement and Analysis," 1388–1401. ACM Press, 2016. https://doi.org/10.1145/2976749.2978313.

Fabre, Cyprien, and Ruth Aggiss. "Cash-Based Response." ECHO. OECD, 2017. https://www.oecd.org/development/humanitarian-donors/docs/cashbasedresponse.pdf.

FAFT. "Guidance on Private Sector Information Sharing." Guidance Document. Paris: Financial Action Task Force (FATF), 2017. www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-information-sharing.html.

"Fake Whatsapp, Instagram, Facebook on the Google Play Store." Deccan Chronicle, January 31, 2017. https://www.deccanchronicle.com/technology/in-other-news/310117/fake-whatsapp-instagram-facebook-on-the-google-play-store.html.

Fifield, David, Chang Lan, Rod Hynes, Percy Wegmann, and Vern Paxson. "Blocking-Resistant Communication through Domain Fronting." *Proceedings on Privacy Enhancing Technologies* 2015, no. 2 (June 1, 2015): 46–64. https://doi.org/10.1515/popets-2015-0009.

"Financial Intelligence Units (FIUs)." The Egmont Group. https://www.egmontgroup.org/en/content/financial-intelligence-units-fius.

Fioretti, Julia. "French Privacy Watchdog Raps WhatsApp over Facebook Data Sharing." *Reuters*, December 18, 2017, Online edition, sec. Technology News. https://www.reuters.com/article/us-whatsapp-privacy-france/whatsapp-faces-french-fine-over-facebook-data-sharing-idUSKBN1EC285.

Flaemig, Tobias, Susanna Sandstrom, Oscar Maria Caccavale, Jean-Martin Bauer, Arif Husain, Arvid Halma, and Jorn Poldermans. "Using Big Data to Analyse WFP's Digital Cash Programme in Lebanon." *ODI Humanitarian Practice Network* (blog), February 20, 2017. https://odihpn.org/blog/using-big-data-to-analyse-wfps-digital-cash-programme-in-lebanon/.

"Fraudulently Issued Security Certificate Discovered." Factsheet. Dutch Cyber Security & Incident Response Team, September 5, 2011. https://goo.gl/4hkYdk.

Fraustino, Julia Daisy, Brooke Liu, and Jan Jin. "Social Media Use during Disasters: A Review of the Knowledge Base and Gaps." Final Report to Human Factors/Behavioral Sciences Division. National Consortium for the Study of Terrorism and Responses to Terrorism (START). College Park, MD: Science and Technology Directorate, U.S. Department of Homeland Security,

December 12, 2012. https://reliefweb.int/report/world/social-media-use-during-disasters-review-knowledge-base-and-gaps.

"Getting Credit - Doing Business." World Bank Group, June 2017. http://www.doingbusiness.org/data/exploretopics/getting-credit.

Gilmour, David. "Meet John Draper, the Phone Phreak Who Inspired Apple's Founders." *The Daily Dot*, October 27, 2017. https://www.dailydot.com/layer8/john-draper-captain-crunch/.

"Government Requests for User Data." Facebook, 2018. https://transparency.facebook.com/government-data-requests.

Greenberg, Andy. "Spies Can Track You Just by Watching Your Phone's Power Use." *Wired*, February 19, 2015, Online edition, sec. Security. https://www.wired.com/2015/02/power-spy-phone-tracking/.

Greenwald, Glenn, Ewen MacAskill, and Laura Poitras. "Edward Snowden: The Whistleblower behind the NSA Surveillance Revelations." *The Guardian*, June 11, 2013, sec. US news. http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance.

GSMA. "Mandatory Registration of Prepaid SIM Cards - Addressing Challenges through Best Practice." GSMA Public Policy. GSMA, April 2016.

———. "State of the Industry Report on Mobile Money." GSMA Mobile Money. GSMA, Bill and Melinda Gates Foundation, Mastercard Foundation, Omidyar Network, 2017. https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2018/02/GSMA_State_Industry_Report_2018_FINAL_WEBv4.pdf.

GSMA Disaster Response. "Towards a Code of Conduct: Guidelines for the Use of SMS in Natural Disasters." GSMA, Souktel, The Qatar Foundation, February 22, 2013. https://www.gsma.com/mobilefordevelopment/programme/mobile-for-humanitarian-innovation/towards-a-code-of-conduct-guidelines-for-the-use-of-sms-in-natural-disasters/.

GSMA Mobile for Development. "Digital Identity Programme." GSMA. https://www.gsma.com/mobilefordevelopment/digital-identity/.

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

Hardesty, Larry. "How Hard Is It to 'de-Anonymize' Cellphone Data?" MIT News, March 27, 2013. https://news.mit.edu/2013/how-hard-it-de-anonymize-cellphone-data.

Harvey, Paul, Katherine Haver, Jenny Hoffmann, and Brenda Murphy. "Delivering Money – Cash Transfer Mechanisms In Emergencies." Cash Learning Partnership (CaLP). London: CaLP; British Red Cross; Oxfam; Save the Children, 2010. http://www.actionagainsthunger.org/sites/default/files/publications/Delivering_Money-Cash_Transfer_Mechanisms_in_Emergencies_03.2010.pdf.

"Home | United Nations Global Pulse." UN Global Pulse. https://www.unglobalpulse.org/.

Hosein, Gus, and Carly Nyst. "Aiding Surveillance: An Exploration of How Development and Humanitarian Aid Initiatives Are Enabling Surveillance in Developing Countries." *SSRN Electronic*

Journal, Privacy International, October 2013. https://privacyinternational.org/report/841/aiding-surveillance.

"How to Use Precise Location on Mobile Devices." Twitter Help Center, 2018. https://help.twitter.com/en/safety-and-security/twitter-location-services-for-mobile.

Hu, Evanna. "Responsible Data Concerns with Open Source Intelligence." *Responsible Data* (blog), November 14, 2016. https://responsibledata.io/2016/11/14/responsible-data-open-source-intelligence/.

ICO. "ICO Submission to the Inquiry of the House of Lords Select Committee on Communications - The Internet : To Regulate or Not to Regulate?" London: Information Commissioner's Office, May 16, 2018. https://goo.gl/9tVzHy.

ICRC. "Cash Transfer Programming (CTP) - Standard Operating Procedures." ICRC Cash Transfer Programming SOP's. ICRC, January 2018. http://webviz.redcross.org/ctp/docs/en/3.%20resources/1.%20Guidance/1.%20Key%20documents/ICRC%20CTP%20SOPs.pdf.

———. "Guidelines for Cash Transfer Programming." Geneva: International Red Cross and Red Crescent Movement, 2007. https://www.icrc.org/eng/resources/documents/publication/pguidelines-cash-transfer-programming.htm.

———. "How to Use Social Media to Engage with People Affected by Crisis." News release. *International Committee of the Red Cross* (blog), October 10, 2017. https://www.icrc.org/en/document/social-media-to-engage-with-affected-people.

———. "Humanitarian Futures for Messaging Apps." Publication. *International Committee of the Red Cross* (blog), January 17, 2017. https://www.icrc.org/en/publication/humanitarian-futures-messaging-apps.

Igoe, Michael. "Facebook Eyes New Partnerships to Better Understand 'High-Risk Areas.'" *Devex*, May 9, 2018, Online edition, sec. Inside Development | Technology. https://www.devex.com/news/sponsored/facebook-eyes-new-partnerships-to-better-understand-high-risk-areas-92721.

Independent Expert Advisory Group, on a Data Revolution for Sustainable Development (IEAG). "A World That Counts – Mobilising the Data Revolution for Sustainable Development." UN Data Revolution. UN Secretary-General, November 2014. http://www.undatarevolution.org/report/.

"Informing Governance with Social Media Mining." Pulse Lab Kampala | UNDP, 2016. https://debates.unglobalpulse.net/uganda/.

Jentzsch, Nicola. "Implications of Mandatory Registration of Mobile Phone Users in Africa." *Telecommunications Policy* 36, no. 8 (September 2012): 608–20. https://doi.org/10.1016/j.telpol.2012.04.002.

Johns Hopkins University. *The Price of Privacy: Re-Evaluating the NSA*. The Johns Hopkins Foreign Affairs Symposium, 2014. https://www.youtube.com/watch?time_continue=1022&v=kV2HD-M86Xgl.

Kemp, Simon. "Digital in 2017: Global Overview." *We Are Social, Hootsuite* (blog), January 24, 2017. https://wearesocial.com/special-reports/digital-in-2017-global-overview.

Khrennikov, Ilya. "Telegram Loses Bid to Block Russia From Encryption Keys." Bloomberg.Com, March 20, 2018. https://www.bloomberg.com/news/articles/2018-03-20/telegram-loses-bid-to-stop-russia-from-getting-encryption-keys.

Kim, Larry. "You Won't Believe All the Personal Data Facebook Has Collected on You." *Medium* (blog), December 7, 2016. https://medium.com/the-mission/you-wont-believe-all-the-personal-data-facebook-has-collected-on-you-387c8060ab09.

Kiselyova, Maria, and Jack Stubbs. "Russia Starts Blocking Telegram Messenger." *Reuters*, April 16, 2018, Online edition, sec. Technology. https://www.reuters.com/article/us-russia-telegram-blocking/russia-starts-blocking-telegram-messenger-regulator-idUSKBN1HN13J.

Kosinski, Michal, David Stillwell, and Thore Graepel. "Private Traits and Attributes Are Predictable from Digital Records of Human Behavior." *Proceedings of the National Academy of Sciences*, March 7, 2013. https://doi.org/10.1073/pnas.1218772110.

Kuner, Christopher, and Massimo Marelli, eds. *Handbook on Data Protection in Humanitarian Action*. ICRC, Brussels Privacy Hub, 2017. www.data-protection-handbook.icrc.org.

"Lessons Learned: Social Media Monitoring during Humanitarian Crises." Geneva: ACAPS, September 21, 2015. https://www.acaps.org/sites/acaps/files/resources/files/lessons_learned-social_media_monitoring_during_humanitarian_crises_september_2015.pdf.

Levin, Avner, Anupa Varghese, and Michelle Chibba. "Know Your Customer Standards and Privacy Recommendations for Cash Transfers." Data Management and Protection. Enhanced Response Capacity Project 2014–2015. UNHCR, Vision International, April 2015. http://www.cashlearning.org/downloads/erc-know-your-customer-web.pdf.

Leyden, John. "SS7 Spookery on the Cheap Allows Hackers to Impersonate Mobile Chat Subscribers." *The Register*, May 10, 2016, Online edition, sec. Security. https://www.theregister.co.uk/2016/05/10/ss7_mobile_chat_hack/.

———. "Whoah! How Many Google Play Apps Want to Read Your Texts?" *The Register*, July 16, 2014, Online edition, sec. Software. https://www.theregister.co.uk/2014/07/16/google_play_app_permissions_too_lax_argues_permission_control_supplier/.

LineageOS. "LineageOS Android Distribution." Lineage. https://lineageos.org/.

Lüge, Timo. "How to Use Social Media to Better Engage People Affected by Crises: A Brief Guide for Those Using Social Media in Humanitarian Organizations." ICRC, IFRC, UNOCHA, September 2017. https://ifrc-1.nyc3.digitaloceanspaces.com/CEASocialmediaguide_WEB_IFRC_EN-.pdf.

Lunt, Andrea. "Messaging Apps: The Way Forward for Humanitarian Communication?" ICRC. *Medium* (blog), July 25, 2017. https://medium.com/law-and-policy/messaging-apps-the-way-forward-for-humanitarian-communication-74ab8f3b113e.

Maas, Paige, Chaya Nayak, Alex Dow, Andreas Gros, Winter Mason, Ismail Onur Filiz, Carlos Diuk, et al. "Facebook Disaster Maps: Methodology." Facebook Research, June 7, 2017. https://research.fb.com/facebook-disaster-maps-methodology.

Marlinspike, Moxie. "Doodles, Stickers, and Censorship Circumvention for Signal Android." *Signal* (blog), December 21, 2016. https://signal.org/blog/doodles-stickers-censorship/.

———. "Open Whisper Systems Partners with Google on End-to-End Encryption for Allo." *Signal* (blog), May 18, 2016. https://signal.org/blog/allo/.

Mas, Ignacio, and Olga Morawczynski. "Designing Mobile Money Services – Lessons from M-PESA." *Innovations: Technology, Governance, Globalization* 4, no. 2 (2009): 77–91.

McCullough, Kimberly. "Why Government Use of Social Media Monitoring Software Is a Direct Threat to Our Liberty and Privacy." *American Civil Liberties Union*, May 6, 2016. https://www.aclu.org/blog/privacy-technology/surveillance-technologies/why-government-use-social-media-monitoring.

Meaker, Morgan. "Europe Is Using Smartphone Data as a Weapon to Deport Refugees." *Wired UK*, July 2, 2018. https://www.wired.co.uk/article/europe-immigration-refugees-smartphone-metadata-deportations.

Mercy Corps. "Cash Transfer Programming Toolkit." Toolkit. Mercy Corps, August 26, 2015. https://reliefweb.int/sites/reliefweb.int/files/resources/mercy_corps_cash_transfer_programming_toolkit_part_1.pdf.

"Messenger Starts Testing End-to-End Encryption with Secret Conversations | Facebook Newsroom." *Facebook Newsroom* (blog), July 8, 2016. https://newsroom.fb.com/news/2016/07/messenger-starts-testing-end-to-end-encryption-with-secret-conversations/.

Montjoye, Yves-Alexandre de, Florimond Houssiau, Piotr Sapieżyński, and Laura Radaelli. "Cambridge Analytica Is Only the Beginning and You Might Have Your Friends to Blame for It." *Computational Privacy Group*, March 29, 2018, CPG, Imperial College London edition. https://cpg.doc.ic.ac.uk/blog/cambridge-analytica-is-only-the-beginning/.

Moody, Chris. "Developer Policies to Protect People's Voices on Twitter." *Twitter Developer Blog* (blog), November 22, 2016. https://blog.twitter.com/developer/en_us/topics/community/2016/developer-policies-to-protect-peoples-voices-on-twitter.html.

Mozur, Paul. "China Presses Its Internet Censorship Efforts Across the Globe." *The New York Times*, March 5, 2018, sec. Technology. https://www.nytimes.com/2018/03/02/technology/china-technology-censorship-borders-expansion.html.

M-PESA. "M-Pesa Customer Terms & Conditions." Safaricom's M-PESA Mobile Money Transfer Service, 2018. https://www.safaricom.co.ke/images/Downloads/Terms_and_Conditions/M-PESA_CUSTOMER_TERMS_AND_CONDITIONS.pdf.

Newberry, Christina. "Social Listening: What It Is, Why You Should Care, and How to Do It Well." Social Media Management. *Hootsuite* (blog), June 13, 2017. https://blog.hootsuite.com/social-listening-business/.

"Number of Monthly Active Twitter Users Worldwide from 1st Quarter 2010 to 2nd Quarter 2018 (in Millions)." Statista, 2018. https://www.statista.com/statistics/282087/number-of-monthly-active-twitter-users/.

"Number of Social Media Users Worldwide 2010-2021." Statista, 2018. https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/.

Osman, Amani. "Social Media E-Learning Course: Sharing the Red Cross and Red Crescent Movement on Social Media." Global Disaster Preparedness Center, 2017. https://www.preparecenter.org/ht/node/17141.

Papaodyssefs, Fotios, Costas Iordanou, Jeremy Blackburn, Nikolaos Laoutaris, and Konstantina Papagiannaki. "Web Identity Translator: Behavioral Advertising and Identity Privacy with Wit." In *Proceedings of the 14th ACM Workshop on Hot Topics in Networks*, 3. ACM, 2015. https://www.recred.eu/sites/default/files/papodyssefs.pdf.

Perlroth, Nicole. "Kazakhstan Moves to Tighten Control of Internet Traffic." *New York Times*, December 3, 2015, sec. Bits Blog. https://bits.blogs.nytimes.com/2015/12/03/kazakhstan-moves-to-tighten-control-of-internet-traffic/.

Poole, Danielle, Mark Latonero, and Jos Berens. "Refugee Connectivity: A Survey of Mobile Phones, Mental Health, and Privacy at a Syrian Refugee Camp in Greece." Signal Program. Harvard Humanitarian Initiative, Data & Society Research Institute, March 2018. http://hhi.harvard.edu/sites/default/files/publications/refugee_connectivity_web.mb4_.8-2.pdf.

Potuck, Michael. "Facebook's 'Protect' Feature on IOS Essentially Installs Spyware on IPhone and IPad." *9to5Mac* (blog), February 13, 2018. https://9to5mac.com/2018/02/13/facebook-protect-spyware-ios/.

"Privacy and Surveillance." ACLU, n.d. https://www.aclu.org/issues/national-security/privacy-and-surveillance.

Privacy International. "Cambridge Analytica and Facebook Are Part of an Industrial Sector That Exploits Your Data." Privacy International, March 20, 2018. http://privacyinternational.org/feature/1681/cambridge-analytica-and-facebook-are-part-industrial-sector-exploits-your-data.

———. "Case Study: Fintech and the Financial Exploitation of Customer Data." Privacy International. http://www.privacyinternational.org/case-studies/757/case-study-fintech-and-financial-exploitation-customer-data.

———. "Case Study: Super-Apps and the Exploitative Potential of Mobile Applications." Privacy International. http://www.privacyinternational.org/case-studies/789/case-study-super-apps-and-exploitative-potential-mobile-applications.

———. "Comments to the Article 29 Working Party Guidelines on Automated Individual Decision-Making and Profiling." Thematic Consultation Submission. Article 29 Working Party Guidelines. Privacy International, November 2017. https://privacyinternational.org/sites/default/files/2017-12/Privacy%20International%20-%20submission%20on%20profiling%20guidance.pdf.

———. "Communications Surveillance." Privacy International, n.d. https://privacyinternational.org/topics/communications-surveillance.

———. "Expose Data Exploitation: Data, Profiling, and Decision Making." Privacy International. https://www.privacyinternational.org/what-we-do/expose-data-exploitation-data-profiling-and-decision-making.

———. "Fintech." Privacy International. https://www.privacyinternational.org/topics/fintech.

———. "Fintech: Privacy and Identity in the New Data-Intensive Financial Sector." Privacy International, November 2017. https://privacyinternational.org/sites/default/files/2017-12/Fintech%20report.pdf.

———. "GCHQ Unlawfully Spied on Amnesty International, Court Admits." Privacy International, July 1, 2015. http://privacyinternational.org/press-release/1156/gchq-unlawfully-spied-amnesty-international-court-admits.

———. "Looking at PRISM - NSA's Mass Surveillance Program." Privacy International, June 7, 2013. http://privacyinternational.org/blog/1363/looking-prism-nsas-mass-surveillance-program.

———. "Middle East and Northern Africa." Privacy International. Accessed July 26, 2018. https://www.privacyinternational.org/location/middle-east-and-northern-africa.

———. "Texas Media Company Hired By Trump Created Kenyan President's Viral 'Anonymous' Attack Campaign Against Rival, New Investigation Reveals." Privacy International, December 15, 2017. http://privacyinternational.org/feature/954/texas-media-company-hired-trump-created-kenyan-presidents-viral-anonymous-attack.

———. "What Is Privacy?" Privacy International. http://www.privacyinternational.org/explainer/56/what-privacy.

"Privacy Policy." Twitter, May 25, 2018. https://twitter.com/content/twitter-com/legal/en/privacy.html.

PwC. "Anti-Money Laundering: Know Your Customer Quick Reference Guide and Global AML Resource Map." PricewaterhouseCoopers, January 2015. https://www.pwc.co.uk/fraud-academy/insights/anti-money-laundering-know-your-customer-quick-ref.html.

"Report Says That SMS Is Not Ideal for Emergency Communications." *Cellular News*, September 16, 2008, Online edition. http://www.cellular-news.com/story/33684.php.

"Resolution on Privacy and International Humanitarian Action." In *37th International Conference of Data Protection and Privacy Commissioners*. Amsterdam, 2015. https://icdppc.org/wp-content/uploads/2015/02/Resolution-on-Privacy-and-International-Humanitarian-Action.pdf.

Rosenbaum, Ron. "Secrets of the Little Blue Box." *Esquire Magazine* 76 (1971): 117–25, 222.

Samenow, Jason. "Why Social Media Would've Saved Lives during Hurricane Katrina." *Washington Post*, August 28, 2015, Online edition, sec. Capital Weather Gang. https://www.washingtonpost.com/news/capital-weather-gang/wp/2015/08/28/why-social-media-wouldve-saved-lives-during-hurricane-katrina/.

Sanders, James. "As Google and AWS Kill Domain Fronting, Users Must Find a New Way to Fight Censorship." *TechRepublic*, May 2, 2018, Online edition, sec. Cyber Security. https://www.techrepublic.com/article/as-google-and-aws-kill-domain-fronting-users-must-find-a-new-way-to-fight-censorship/.

Sayer, Peter. "German Court Upholds WhatsApp-Facebook Data Transfer Ban." *PCWorld*, April 26, 2017, Online edition, sec. News. https://www.pcworld.com/article/3192614/privacy/german-court-upholds-whatsapp-facebook-data-transfer-ban.html.

"Security." Viber. https://www.viber.com/security/.

"Sharing Your Data with Twitter's Business Partners." Twitter. https://help.twitter.com/en/safety-and-security/data-through-partnerships.

Smith, Gabrielle, Ruth McCormack, Alex Jacobs, Arushi Chopra, Aarsh Vir Gupta, and Thomas Abell. "The State of the World's Cash Report – Cash Transfer Programming in Humanitarian Aid." Full Report. CaLP, Accenture, February 2018. http://www.cashlearning.org/downloads/calp-sowc-report-exs-web.pdf.

"Social Media – Statistics & Facts." Statista, 2018. https://www.statista.com/topics/1164/social-networks/.

"Social Media and Forced Displacement: Big Data Analytics & Machine-Learning." White Paper. UNHCR Innovation Service, UN Global Pulse, September 2017. http://www.unhcr.org/innovation/wp-content/uploads/2017/09/FINAL-White-Paper.pdf.

"Social Media for Good." *Sm4good* (blog). http://sm4good.com/.

"Social Media in Emergencies." *UNHCR | Emergency Handbook* (blog). https://emergency.unhcr.org/entry/168552/social-media-in-emergencies.

Sottek, T. C., and Janus Kopfstein. "Everything You Need to Know about PRISM." *The Verge*, July 17, 2013, Online edition, sec. Policy and Law. https://www.theverge.com/2013/7/17/4517480/nsa-spying-prism-surveillance-cheat-sheet.

"SQuid: Humanitarian Aid & Development." Humanitarian Aid and Development. https://www.squidcard.com/products-solutions/humanitarian-aid-development.

Steel, Emily, and Geoffrey A. Fowler. "Facebook in Privacy Breach." *Wall Street Journal*, October 18, 2010, sec. Tech. http://www.wsj.com/articles/SB10001424052702304772804575558484075236968.

Su, Jessica, Ansh Shukla, Sharad Goel, and Arvind Narayanan. "De-Anonymizing Web Browsing Data with Social Networks." In *Proceedings of the 26th International Conference on World Wide Web*, 1261–69. Perth, Australia: International World Wide Web Conferences Steering Committee, 2017.

Swichkow, Brian. "How I Pranked My Roommate With Eerily Targeted Facebook Ads." Ghost Influence, September 6, 2014. http://mysocialsherpa.com/the-ultimate-retaliation-pranking-my-roommate-with-targeted-facebook-ads/.

Timberg, Craig. "For Sale: Systems That Can Secretly Track Where Cellphone Users Go around the Globe." *Washington Post*, August 24, 2014, Online edition, sec. Technology. https://www.washingtonpost.com/business/technology/for-sale-systems-that-can-secretly-track-where-cellphone-users-go-around-the-globe/2014/08/24/f0700e8a-f003-11e3-bf76-447a5df6411f_story.html.

Toor, Amar. "Germany Moves to Seize Phone and Laptop Data from People Seeking Asylum." *The Verge*, March 3, 2017, Online edition. https://www.theverge.com/2017/3/3/14803852/germany-refugee-phone-data-law-privacy.

"Transparency Report." Twitter, 2018. https://transparency.twitter.com/en.html.

Traynor, Patrick. "Characterizing the Security Implications of Third-Party Emergency Alert Systems over Cellular Text Messaging Services." In *Security and Privacy in Communication Networks*, edited by Sushil Jajodia and Jianying Zhou, 50:125–43. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010. https://doi.org/10.1007/978-3-642-16161-2_8.

Turken, Iffet. "The Power of Social Media When Disaster Strikes." Strategy. *INSEAD Knowledge* (blog), September 21, 2017. https://knowledge.insead.edu/blog/insead-blog/the-power-of-social-media-when-disaster-strikes-7201.

"UAE National PKI Repository." DarkMatter, June 2016. https://ca.darkmatter.ae/UAE/index.html.

UK Information Commissioner's Office. "Big Data, Artificial Intelligence, Machine Learning and Data Protection." Data Protection Act and General Data Protection Regulation, September 2017. https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf.

UNCTAD. "Mobile Money for Business Development in the East African Community – A Comparative Study of Existing Platforms and Regulations." ICT Analysis Section. UNCTAD, 2012. http://unctad.org/en/PublicationsLibrary/dtlstict2012d2_en.pdf.

UNHCR. "From a Refugee Perspective – Discourse of Arabic Speaking and Afghan Refugees and Migrants on Social Media from March to December 2016." Regional Bureau for Europe – Communicating with Communities Unit. UNHCR, April 2017. http://www.unhcr.org/publications/brochures/5909af4d4/from-a-refugee-perspective.html.

UNOCHA. "Social Media Monitoring." Guidance. HumanitarianResponse. https://www.humanitarianresponse.info/en/applications/tools/category/social-media-monitoring.

vijay. "How To Hack WhatsApp Using SS7 Flaw." *TechWorm* (blog), June 2, 2016. https://www.tech-worm.net/2016/06/how-to-hack-whatsapp-using-ss7-flaw.html.

Vinck, Patrick, Anne Bennett, and Jacobo Quintanilla. "Engaging with People Affected by Armed Conflicts and Other Situations of Violence – Taking Stock. Mapping Trends. Looking Ahead. Recommendations for Humanitarian Organizations and Donors in the Digital Era." ICRC, Harvard Humanitarian Initiative, February 2018. https://www.icrc.org/en/publication/engaging-people-affected-armed-conflicts-and-other-siutations-violence.

Vines, Paul, Franziska Roesner, and Tadayoshi Kohno. "Exploring ADINT: Using Ad Targeting for Surveillance on a Budget - or - How Alice Can Buy Ads to Track Bob," 153–64. ACM Press, 2017. https://doi.org/10.1145/3139550.3139567.

Wadhwa, Vivek. "WhatsApp Public Groups Can Leave User Data Vulnerable to Scraping." *VentureBeat*, April 3, 2018. https://venturebeat-com.cdn.ampproject.org/c/s/venturebeat.com/2018/04/03/whatsapp-public-groups-can-leave-user-data-vulnerable-to-scraping/amp/.

Wagner, Ben. *After the Arab Spring: New Paths for Human Rights and the Internet in European Foreign Policy*. Directorate-General for External Policies of the Union. Luxembourg: European Parliament, 2012. http://bookshop.europa.eu/uri?target=EUB:NOTICE:BB3212238:EN.

Walker, Tom. "Humanitarian Futures for Messaging Apps - Understanding the Opportunities and Risks for Humanitarian Action." ICRC, The Engine Room, Block Party, January 2017. www.icrc.org/en/document/messaging-apps-untapped-humanitarian-resource.

Warnes, John. "Using Data to Make Your Humanitarian Organisation More Client-Focused." *UNHCR Innovation Service*, 2017.

"What Are Skype Private Conversations?" Skype Support. https://support.skype.com/en/faq/FA34824/what-are-skype-private-conversations.

"What Is a Software Library? - Definition from Techopedia." Techopedia.com. https://www.techopedia.com/definition/3828/software-library.

"WhatsApp Data Protection Act Undertaking." Data Protection Act 1998. Information Commissioner's Office; WhatsApp, March 12, 2018. https://ico.org.uk/media/action-weve-taken/undertakings/2258376/whatsapp-undertaking-20180312.pdf.

"WhatsApp Legal Info." WhatsApp.com, April 24, 2018. https://www.whatsapp.com/legal/#privacy-policy-information-you-and-we-share.

Williams, Matthew L., Pete Burnap, Luke Sloan, and Curtis Jessop. "Practice Note Using Social Media Data in International Development Research, Monitoring & Evaluation." NatCen Social Research. London: UK Department for International Development, August 2016. https://assets.publishing.service.gov.uk/media/57d968c540f0b6533a000052/Social_Media_DFID_Practice_Note_PDF_September_2016_Emily_Poskett.pdf.

World Bank. "Identification for Development - Strategic Framework." ID4D. World Bank, January 25, 2016.

York, Jillian C., and Trevor Timm. "Surveillance Inc: How Western Tech Firms Are Helping Arab Dictators." *The Atlantic*, March 6, 2012, Online edition. https://www.theatlantic.com/international/archive/2012/03/surveillance-inc-how-western-tech-firms-are-helping-arab-dictators/254008/.

Yoshikawa, Lynn. "Integrating Cash Transfers into Gender-Based Violence Programs in Jordan: Benefits, Risks and Challenges." Enhanced Response Capacity Project 2014–2015. International Rescue Committee, February 1, 2016. http://www.cashlearning.org/resources/library/827-integrating-cash-transfers-into-gender-based-violence-programs-in-jordan-benefits-risks-and-challenges-?keywords=&region=all&country=all&year=all&organisation=all&sector=all&modality=all&language=all&payment_method=all&document_type=all&searched=1.

"Your Twitter Data." Twitter. https://twitter.com/settings/your_twitter_data.

Youyou, Wu, Michal Kosinski, and David Stillwell. "Computer-Based Personality Judgments Are More Accurate than Those Made by Humans." *Proceedings of the National Academy of Sciences* 112, no. 4 (January 27, 2015): 1036–40. https://doi.org/10.1073/pnas.1418680112.

Zanon, Gregorio. "No, End-to-End Encryption Does Not Prevent Facebook from Accessing WhatsApp Chats." *Medium* (blog), April 12, 2018. https://medium.com/@gzanon/no-end-to-end-encryption-does-not-prevent-facebook-from-accessing-whatsapp-chats-d7c6508731b2.

Zenz, Kimberly. "Russia Accidentally Sabotages Its Internet." *The Daily Beast*, April 19, 2018, Online edition. https://www.thedailybeast.com/russia-accidentally-sabotages-its-internet.

Zuckerberg, Mark. "An Update on the Cambridge Analytica Situation." Facebook post. Facebook, March 21, 2018. https://www.facebook.com/zuck/posts/10104712037900071.

Court Cases

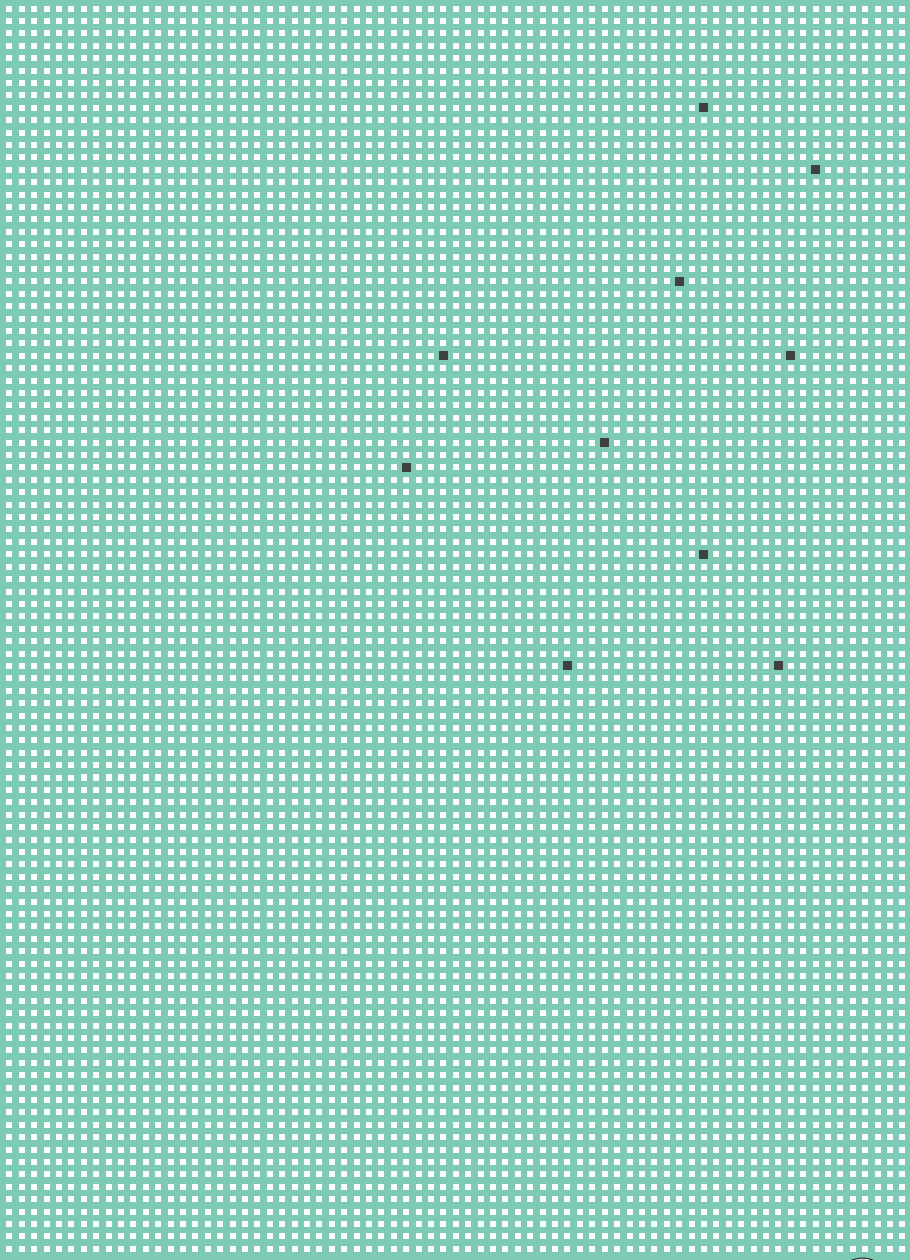
Investigatory Powers Tribunal (IPT), Determination [2015], UKIPTrib 13_77-H_2, Case N.: IPT/13/77/H, IPT/13/92/CH, IPT/13/168-173/H, IPT/13/194/CH, IPT/13/204/CH, London, 22 July 2015.

P.G. and J.H. v. the United Kingdom, Application no. 32792/05, ECHR Judgement, 25 December 2001.

Vukota-Bojić v. Switzerland, Application no. 61838/10, ECHR Judgement, 18 October 2016.

Perry v United Kingdom, Merits, Application no. 63737/00, ECHR, 17 July 2003.

Peck v the United Kingdom, Application no. 44647/98, ECHR Judgement, 28 January 2003.



PRIVACY INTERNATIONAL

ICRC