IOM UN MIGRATION
OCHA
centre for humdata
IFRC
ICRC

TIP SHEET ON MAINTAINING CONFIDENTIAL DIGITAL DIALOGUE DURING HUMANITARIAN EMERGENCIES

***Disclaimer:** This document is not intended to replace official organizational guidance or security rules. The advice it contains is designed to cover situations where it may not be possible to rely on corporate tools or established procedures. Users are responsible for ensuring that any use of digital communications tools or security measures (such as a VPN) is lawful. This document does not supersede or substitute any applicable policies, regulations, legal requirements or rules of organizations, and humanitarian staff should always seek further advice from appropriate colleagues as necessary.*

INTRODUCTION

Confidentiality is of fundamental importance in humanitarian settings, as it is an essential precondition for carrying out humanitarian operations. For example, humanitarian action is often dependent upon the maintenance of confidential dialogue with parties to a conflict or key actors in other humanitarian environments. This dialogue may be necessary to gain access to affected populations, facilitate movement through territory controlled by non-state actors or negotiate in support of planning and executing humanitarian programming. In some cases, it may also be necessary to maintain a confidential dialogue with affected populations to ensure they can access humanitarian services in ways that do not expose them to harm. Similarly, confidential communications between humanitarian partners, as well as among humanitarian partners and affected populations, are critical to humanitarian action.

Maintaining the confidentiality, integrity and authenticity of communications is essential in these situations. Humanitarian actors will have often spent many years establishing and building the trust of interlocutors. Breaches of confidentiality could undermine these relationships, with potentially harmful consequences for affected populations. Were the breach to present – or be perceived to present – an advantage to opposing parties to an armed conflict or adversaries in other situations of violence, it could also pose a very real threat to the safety of humanitarian workers and the continued provision of humanitarian services. Such events could also threaten the perception of neutrality and impartiality of humanitarian actors.

Many interlocutors are already well aware of the risks of surveillance and intelligence-gathering and have developed working methods to maintain confidentiality. In-person meetings with authorities or affected people have traditionally allowed organizations to obtain and protect confidential information or sensitive personal data.

The current COVID-19 health crisis, with its movement restrictions and social distancing rules, makes in-person meetings difficult to arrange. Maintaining contact with affected populations, other humanitarian partners, parties to a conflict and other interlocutors is increasingly reliant on digital communications, e.g. instant messaging, videoconferencing and email. More generally, with digital communications becoming more common in humanitarian work, confidentiality and the secure transfer of information and data via digital means is essential.

This tip sheet offers:

- an overview of the threats to confidentiality associated with digital communications in higher risk humanitarian contexts, including physical and covert surveillance, metadata, interception and hacking
- recommendations to mitigate those threats, including communication protocols, countermeasures, digital security, choice of application and digital hygiene
- a set of resources that can be used to help identify suitable communications tools.

1. THREATS

In humanitarian contexts there is a higher likelihood that individuals and whole population groups will be the subject of surveillance by a variety of actors, including governments and their proxies. In the current COVID-19 health crisis, new surveillance capacities are being introduced as part of the response in some contexts. The threat to the confidentiality of sensitive information and personal data collected by humanitarian organizations will vary from one country to the next, but some risks are present regardless of location.

PHYSICAL & COVERT SURVEILLANCE

- Anyone within the vicinity of a meeting, from bystanders to passers-by, could be a human intelligence (or “HUMINT”) source.
- Covert surveillance devices or “bugs”, including voice and audio recorders, are cheap and easy to use.
- Video cameras with audio recording and real-time transmission capability are getting smaller, cheaper and easier to conceal.

DIGITAL SURVEILLANCE

- All digital activities leave so-called digital footprints on devices, servers and network infrastructure.
- These tracks consist of metadata (that is, data about data), which is generated to a greater or lesser extent by all digital applications.
- Metadata can be obtained via open-source methods as well as via intrusive means.
- Metadata gathered from social media and other open-access platforms can be used by adversaries to identify targets for further surveillance.
- Even when unique identifiers are removed from metadata, it can still lead to re-identification of individuals or groups.
- Surveillance of telecommunication networks can happen locally, by eavesdropping on poorly secured Wi-Fi networks (akin to wiretapping a landline telephone), or at the national level, where telecommunication service providers may be under a legal obligation to provide government agencies with access to communications being transmitted through their infrastructure.
- This kind of surveillance may take place in real time or by analysing past communications.
- Local network surveillance may be conducted by the network owner or an unauthorized third party with access to the network.
- Such techniques may enable those conducting the surveillance to identify and profile devices, users of a network, their geographic location and the people they have communicated with.

DEVICE & APPLICATION VULNERABILITIES

- Many devices are sold with applications that readily enable surveillance, including tools enabling the browsing of the device's content, the tracking of contacts, applications to find lost devices, and activity tracking tools, all of which may transmit geolocation data to third parties in real time.
- Free applications are often predicated on a business model that exploits personal data, creating vulnerabilities.
- The default settings of secure messaging applications may also contain inherent vulnerabilities, such as setting message encryption to 'off' cloud back-ups to 'on' and enabling conference recording, which store conversations on third-party servers.
- Such vulnerabilities may render devices and applications more susceptible to eavesdropping, interception and other forms of surveillance.

INTERCEPTION

- All communications channels are vulnerable to interception.
- Analogue communications, including landline telephones and radio, are unencrypted and relatively easy to intercept by a capable adversary.
- Email is particularly vulnerable to interception. While email services may use encryption and other controls to reduce risks related to message transmission, a communication channel is only as secure as the weakest link in the chain, be it the user, the device or one of many service providers.
- Targeted state surveillance, facilitated by telecommunication service providers, may enable security agencies to access the content of private communications.
- State and non-state actors may also use tools known as "IMSI-catchers" that masquerade as legitimate cell phone towers to eavesdrop on mobile phone communications.

UNAUTHORIZED ACTIVITIES & REMOTE ACCESS

- Local law enforcement and security agencies may be authorized to monitor devices, device data and device application activities.
- Foreign intelligence agencies may target parties to a conflict and key interlocutors under cyber espionage mandates.
- The market for surveillance and surveillance tools is booming, providing state and non-state actors with a wide range of techniques to access computer devices.
- Less technical approaches, such as impersonation via social engineering, also pose a serious threat to individuals and organizations. These approaches can include the use of deception to manipulate individuals into divulging confidential or personal information.
- Vulnerable, poorly configured or outdated software can be exploited for surveillance purposes.
- "Phishing" attacks that convince individuals to click on a link in communications that appear to have come from trusted sources can enable remote access to a device or compromise its contents.
- Malware may be installed on a device from compromised links sent via SMS or messaging applications, emails and attachments.
- Local legislation may compel service providers and software vendors to provide national governments with interception or encryption backdoors.
- These vulnerabilities can be exploited by state and non-state actors alike.

While the risk profile of any specific humanitarian dialogue will vary from one situation to the next, these threats must be taken into account. Where there is a strong likelihood that dialogue may be targeted for surveillance and compromised, this could have very serious repercussions for the parties involved. Irrespective of the situation, however, humanitarian actors should strive to minimize the risk of breaches of confidentiality to the fullest practical extent.

2. RECOMMENDATIONS

Although there is no such thing as risk-free communication, particularly in digital environments, even rudimentary knowledge of the threats, low-tech precautions, basic digital hygiene and careful selection of software and hardware provider can minimize exposure to surveillance and interception.

Establish a communications protocol

- Make communications security a fundamental component of your dialogue.
- Determine when, how and what communications tools are to be used while considering the local context.
- Be prepared to support interlocutors and affected populations in understanding, configuring and using secure digital tools.
- Use techniques to confirm identity and confidentiality of communications, including by exchanging codewords and phrases known only to the parties to the dialogue at the start of the communication.
- Prefer messaging applications that allow verification of counterparties (e.g. via QR codes).
- Have a backup plan in case the primary means of communication is compromised or unavailable.
- Be ready to abort the communication and maintain the ability to notify other parties if the confidentiality or authenticity of the communication is in doubt.

Your local surroundings

- Check there is no-one in your vicinity able to eavesdrop on your conversation. If you are concerned about eavesdropping in your office, vehicle or place of residence, find an alternative location from which to communicate. Use a (removable) privacy screen to prevent your display from being seen by anyone in your vicinity or by surveillance cameras, especially when working in public places.
- If using a video conferencing application, avoid revealing unnecessary information such as your location, for example by using a background image or by removing distinctive objects from desks, walls, etc. Use your camera when video conferencing only if it is necessary.

Network security

- Be wary of public or open Wi-Fi networks. (i.e. those without a password and usually free of charge).
- Where possible, use your mobile phone as a hotspot to avoid untrusted Wi-Fi networks.
- If you do need to use a public Wi-Fi network, verify the identity of the provider (e.g. the café or restaurant) and access it via a virtual private network (VPN).

Encryption

- Use messaging and voice calls that provide end-to-end encryption.
- Avoid video conferencing applications as far as possible, as features such as end-to-end encryption are seldom available. If videoconferencing is necessary, limit participation to one-to-one communication, where such features may be available and effective, and ensure they are enabled and active during your call.

Device security

- Learn more about threats to data protection, information and device security by completing available training and familiarizing yourself with all relevant guidance provided by your organization.
- If you are using your own device for confidential communications:
  - ensure the operating system and all the applications that you use are up to date.
  - register your device with your organization's mobile device management system. This will help to protect your device against malware and insecure communication channels and will ensure your data are protected in the event of loss or theft.
  - if your organization does not offer a mobile device management system, ensure your device has the encryption features activated and consider installing a mobile anti-malware application.
  - prevent popular applications from using device features that are not strictly needed, such as location tracking, camera and microphone.
- If any functions or applications are behaving suspiciously, or if you are concerned that your device may have been compromised, seek advice and assistance from experts.

Choice of application for communication

- Use only the devices and applications provided and authorized by your organization. If circumstances require the use of other devices or applications, follow any applicable rules or guidance from your organization.
- Consult knowledgeable colleagues and/or up-to-date analysis of the security features and risks associated with different communications tools to identify the most appropriate application for the country and environment in which the dialogue is to take place (see Resources below).
- Avoid using emails or social-media platforms for any sensitive humanitarian dialogue.
- Install only verified applications from official sources.
- Ensure that your chosen application can be used by your interlocutors, for example by checking that they have the device, connectivity and level of expertise to use it securely.
- Ensure that the application selected is already used widely enough in the country to avoid the risk that by downloading it you or your interlocutor could be attracting attention.
- Prefer applications with end-to-end encryption features to help minimize the risks of interception or eavesdropping.
- Select applications that have the lightest digital footprint and produce only the metadata necessary for the application to function.
- Prefer applications that have been thoroughly and independently audited by the security research community. In general, such applications have a higher degree of transparency and may be considered less likely to contain hidden malware or backdoors for unauthorized access, compared to commercial (often closed-source) alternatives.
- Select applications that support multifactor authentication, and enable this wherever possible.
- Prefer applications that provide end-to-end video and voice-call encryption if you need to verify the physical identity of your interlocutor.
- Learn about the risks posed by videoconferencing applications in the Tip Sheet on the Responsible Use of Online Conferencing Tools.
- In high-risk situations, consider using a dedicated device with a high-security configuration.

Digital hygiene

- Verify device and application backup configuration to ensure device and application data are not insecurely or unduly transferred to other locations.
- Consider using message auto-deletion feature where available and appropriate.
- Avoid installing or using popular applications that contain known security vulnerabilities.

If in doubt

- Following these recommendations as far as is practical should provide an adequate level of communications security in most contexts.
- However, for the most sensitive dialogue in high-risk situations, the residual risks may render any form of digital communication unsuitable.
- In these scenarios, there may be no viable substitute for in-person meetings or traditional forms of communication, such as courier messages from interlocutors.

3. RESOURCES

- *Citizen Lab, Security Planner:* https://securityplanner.org/#/
- *Electronic Frontier Foundation, Surveillance Self-Defense: Tips, Tools and How-to's for Safer Online Communications:* https://ssd.eff.org/en
- *Freedom of the Press Foundation, Guides & Training:* https://freedom.press/training/
- *ICRC Data Protection Office, IFRC & OCHA Centre for Humanitarian Data, Tip Sheet on the Responsible Use of Online Conferencing Tools:* https://www.icrc.org/en/publication/tip-sheet-responsible-use-online-conferencing-tools
- *Privacy International and the ICRC, The Humanitarian Metadata Problem: "Doing No Harm" in the Digital Era:* https://www.icrc.org/en/download/file/101039/final_web_the_humanitarian_metadata_problem_-_doing_no_harm_in_the_digital_era.pdf *Secure Messaging Apps Comparison:* https://www.securemessagingapps.com/

facebook.com/icrc
twitter.com/icrc
instagram.com/icrc

International Committee of the Red Cross
19, avenue de la Paix
1202 Geneva, Switzerland
T +41 22 734 60 01
shop.icrc.org

International Organization for Migration
17 Route des Morillons
1218 Grand-Saconnex
Switzerland

Centre for Humanitarian Data
UN Office for the Coordination
of Humanitarian Affairs
Fluwelen Burgwal 58
2511 CJ, The Hague, The Netherlands
centre.humdata.org

International Federation of Red Cross
and Red Crescent Societies
Chemin des Crêts 17
Petit-Saconnex 1209 Geneva
Switzerland
Ifrc.org

4481/002 06.2020