Digital Democracy

Threats faced by earth defenders and their data, and implications for tech development

Report compiled by Aliya Ryan, based on research carried out by the Digital Democracy Team

Photo by Digital Democracy

Research made possible by support from Open Technology Fund

May 2023

Preface

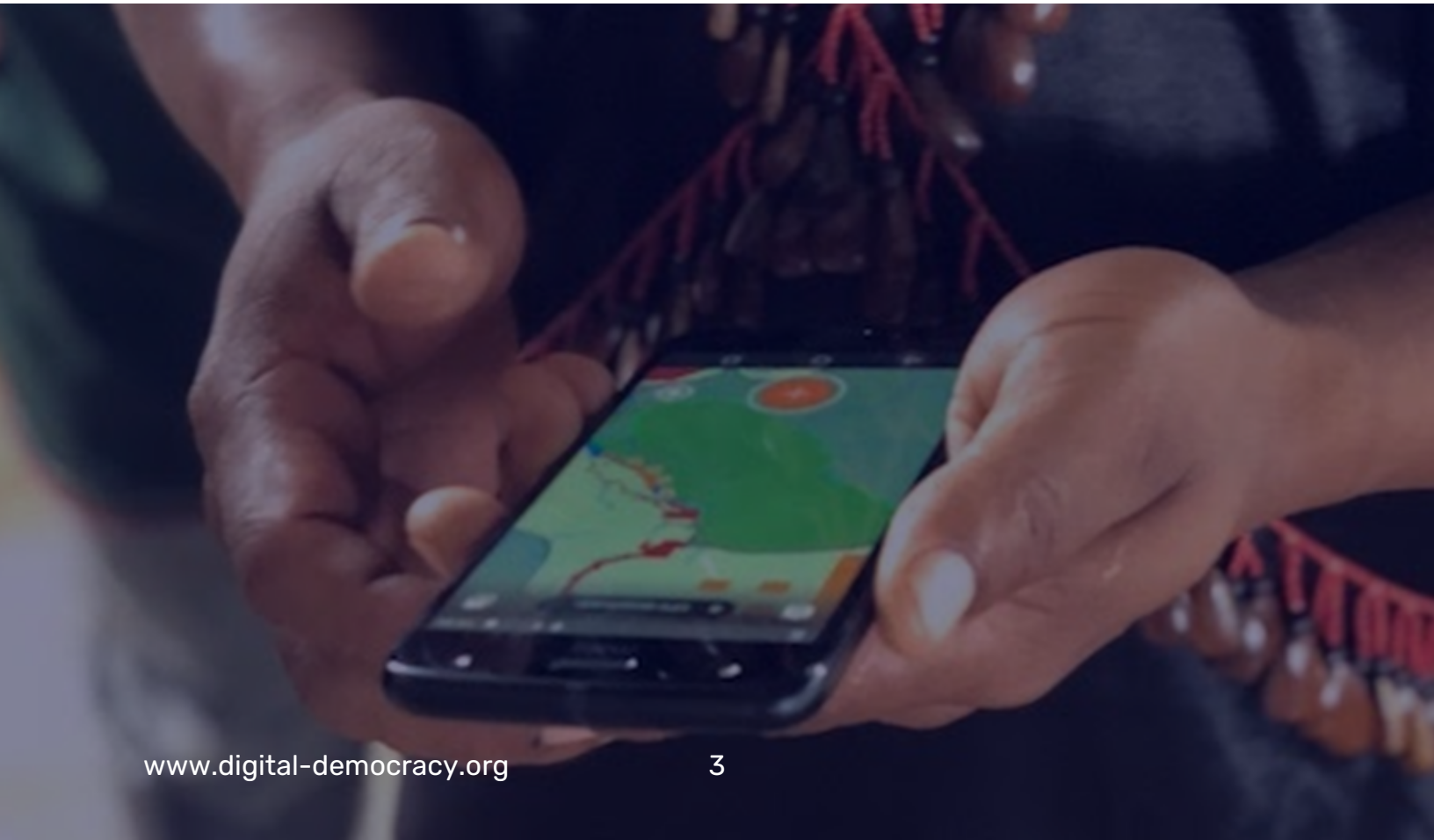
To the earth defenders, who every day put love for the land, justice, their heritage and their children's futures before all else.

Bruno Pereira was one such defender, who some of our team had the privilege of working with, and who was murdered in June 2022 whilst working on exposing illegal fishing activities in the Brazilian Amazon.

It is impossible to start a report compiling research on the topic of security concerns for earth defenders without acknowledging the price he — and far too many environmental and human rights defenders — have paid for doing their work, and the impacts this violence has on their families, communities, colleagues and the land.

This report is based on the lived experiences and aggressions reported to our team by many individuals. We thank you for your time and trust in sharing with us.

Table of Contents



1: Introduction

1.1 Background and Objectives

This report discusses the findings of interviews done between 2020–2022 with Indigenous environmental and human rights defenders and their allies living and working within oppressive regimes. The interviews explored the diversity of threats they face and their security needs, in order to improve the interfaces and features of Mapeo — an app for documenting environmental and human rights abuses. The findings are guiding technical development work on Mapeo, to guard against vulnerabilities occurring due to physical device seizure and surveillance. We hope that the report will also be useful to technologists and others working with similar users or in similar contexts around the world. The research and report was made possible by a contract with Open Technology Fund.

Mapeo is an open source toolkit designed by Digital Democracy in partnership with Indigenous communities for the collaborative documentation of environmental and human rights abuses, with photos linked to geographic information and cryptographic proofs. Mapeo is resilient during censorship, blackout, and with limited or no connectivity, as data can be collected and shared offline between devices. The local-first database does not require any setup and is embedded in the mobile and desktop apps.

Digital Democracy has many years of experience working with frontline communities in the Amazon region, and has developed Mapeo alongside Indigenous communities to directly meet their needs. Over the last few years we have received numerous requests for support implementing Mapeo from frontline earth defenders and human rights activists around the world, in particular in Brazil, South East Asia and Sub Saharan Africa. These groups are often working in oppressive contexts where they, and their data, are under threat. Research by Global Witness revealed that in 2020, an average of over four people were killed per week globally for their work defending land, livelihoods and the environment[1], with over 50% of

[1] Global Witness 2021, Last Line of Defence, https://www.globalwitness.org/en/campaigns/environmental-activists/last-line-defence/

these coming from countries included within this research, governed by repressive regimes.

To respond to requests from these groups, we must ensure that Mapeo meets their security needs, and in order to do this we need a better understanding of their requirements and the contexts they live and work within. In particular we would like to understand how low technical literacy and limited access to the internet or phone networks could constrain or impact potential security implementations.

For ease of reading, the term *earth defender* is used at times in this report, in addition to *environmental and human rights defenders,* to refer to the protagonists of this critical and dangerous work.

1.2 Security Situation of Environmental and Human Rights Defenders

The UN defines environmental land rights defenders as "individuals and groups who, in their personal or professional capacity and in a peaceful manner, strive to protect and promote human rights relating to the environment, including water, air, land, flora, and fauna". These people are often on the frontlines of social and environmental struggles, working to combat challenges including: climate change; land invasions; deforestation; extractive industries including mining and oil exploitation; illegal fishing and hunting; dam construction; and encroachments onto their ancestral or customary lands for agriculture, conservation, tourism or other reasons.

The areas earth defenders live in are frequently areas of conflict over land or resources. Their work therefore often brings them into opposition to powerful companies, governments or other agents, from whom they might face open or covert threats and intimidation, which might lead to violence or even assassination. Earth defenders may be criminalized, as governments create laws that outlaw their activities (e.g. protests, visiting border areas, etc.)or create phony lawsuits to hinder their work or waste time, and earth defenders might face unlawful detentions and experience violence while in detention.

As part of their work, some groups of earth defenders collect evidence about environmental or human rights abuses, often using smartphones and a range of applications, including Mapeo, to record evidence. The incorporation of digital tools into earth defenders' work, whilst providing benefits for data collection, can also place them at further risk. They might be targeted whilst in location, collecting evidence or data, or their devices might be confiscated or stolen, with valuable and sensitive information being lost or falling into the wrong hands. Their use of technology could also increase the ease with which governments, companies, and others are able to track, follow, and collect information about them without their knowledge. Our research has shown it is commonplace for earth defenders to have their phones and devices tapped, hacked, and tracked.

2: Research Methods

2.1 Who and How

The research published in this report was carried out through a series of interviews, focus groups and workshops from June 2020 to June 2022. We had intended to conduct some of these in-person during field trips to Brazil and South East Asia, but due to the travel and other restrictions of the COVID-19 pandemic they all happened remotely.

Digital Democracy developed a semi-structured interview template, which was customized for each participant, with open questions relating to technical literacy, connectivity and physical, digital and other security vulnerabilities. Interviewees had freedom to follow lines of enquiry as they emerged, depending on the local contexts and particular experiences of the participants.

Participants came from 14 civil society organizations, including Indigenous peoples and community members involved in documentation of environmental and human rights abuses, coordinators who manage data, and trainers and advocates with experience in digital security and monitoring and mapping techniques.

In order to ensure the safety of participants and respect their anonymity, information which could identify the individuals and their organizations is being excluded from this report, however the spread of the research participants is summarized below.

Total number of participants: 26 (16 men and 10 women)including 11 Indigenous peoples, and coming from 14 civil society organizations.

Geographic spread: Sub Saharan Africa (11); Southeast Asia (2); Brazil (11); Northwestern Amazon (2)

Roles: Data collector/Monitor (9); Organizer/Coordinator (7); Trainer/Advocate/Researcher (10)

The Numbers

In order to ensure the safety of participants and respect their anonymity, information which could identify the individuals and their organizations is being excluded from this report, however the spread of the research participants is summarized below:

Roles

Data collector/Monitor (9)
Organizer/Coordinator (7)
Trainer/Advocate/Researcher (10)

Geographic Spread

Sub Saharan Africa (11)
Southeast Asia (2)
Brazil (11)
Northwestern Amazon (2)

Number of Participants

26 (16 men and 10 women) including 11 Indigenous peoples, and coming from 14 civil society organizations

Interviewee Profiles

The profiles below are created by amalgamating characteristics from various interviewees so as to give readers unfamiliar with frontline environmental and human rights defenders a sense of their work and the contexts they work within, whilst keeping individual stories anonymous. These only represent a small number of the situations and realities of our interviewees, whose wide views and experiences are more fully discussed in Section 3.

A data collector:

A*** lives in a small, Indigenous village on the edge of a mangrove forest, with no mobile phone coverage or internet. She has been trained by her representative organization to collect mapping data about her people's ancestral and customary land use for a legal case, and to document illegal fishing activities she encounters. A*** goes on monthly trips with 3-4 other members of the mapping team to collect data, and every three months comes to a central location to share this data with her organization. If her team discovers any serious illegal activity they will walk a day to a village with internet to send an alert over whatsapp with photos and documentation to their organization. She shares a mobile phone with her parents and siblings, there is no passcode on the phone and twice she has lost data through water damage to the phone caused when someone else was using it.

An organizer:

B*** is an Indigenous leader, living and working within their village high on a mountain, and coordinating their people's opposition to new agricultural developments on their land, as well as monitoring the impacts of nearby mining activities. There is intermittent internet and phone signal available from a few public locations in the village. B*** is in charge of the team of defenders, collating and sharing the information they collect with other leaders and decision makers, and when needed publishing it on social media. B*** often accompanies the teams when they go out to collect evidence of illegal activities, and has been involved in numerous confrontations with illegal land invaders, as well as with armed contractors from the mining company. B***'s organization has a well developed security protocol for data collection missions, developed after two individuals were attacked whilst out on a mission, and individuals now never go out alone. However even so B*** has been

personally threatened on numerous occasions, has spent two weeks in jail on made-up charges, which were later dropped, and suspects his phone is being tapped by the mining company.

A trainer:

C*** is non Indigenous and lives and works for a national level NGO in the country's capital. They provide frontline earth defenders with advice on how to organize against illegal resource extractors, connect Indigenous organizations with legal resources and are in charge of a number of campaigns against national companies involved in oil and gas extraction on Indigenous lands. C*** also runs trainings in a variety of data collection techniques and apps. C*** frequently receives photos and other evidence of environmental rights violations from the organizations they work with via whatsapp, facebook messenger, telegram and email, and stores this all in a google drive. Generally C*** does not feel personally threatened, although once when working on a high profile international case their NGO's offices were raided and their laptop was stolen. However C*** knows many Indigenous and other frontline leaders who have been attacked including one who was recently murdered. The NGO they work for is supporting two individuals who have gone into hiding for their own safety after speaking out against illegal activities.

2.2 Ethics

Carrying out interviews with Indigenous community members, earth defenders and those that work with them raises a series of ethical questions that we set out to address when developing our research methodology.

Many of our interview subjects have historically been subject to diverse forms of extractivism and colonialism, and we recognise that participating in the interviews was a demand on their time, in addition to the value of the views and experiences they shared. Participant organizations were remunerated for their time and other costs involved in participating in the research.

We were also careful to only involve organizations that either knew us directly, and trusted us, our methods and objectives, or organizations introduced to us by mutually trusted third

parties. We are grateful for all the insights and information shared with us by the participants, and acknowledge that monetary remuneration only covers some aspects of the value of their contributions.

As stated in section 1.2, earth defenders are often the target of powerful groups, agencies and companies and many face physical and other threats as part of their working life, particularly those living within oppressive regimes and contexts, as was the case with our interviewees.

To ensure the identities of the interviewees are kept secure and that their participation in this research did not add to the risks they face, all interviewees and their organizations are anonymized in this report. When referenced we have done so with codes (Source 1, 2 etc.) rather than use their names, and we avoid providing information that could result in their identification. In some cases this may lead to the anecdotes or evidence provided in this report appearing vague or unspecific, however it was a necessary step to protect our sources.

We also deleted video or audio recordings of the interviews once notes had been compiled, and stored any notes in a restricted folder.

2.3 Changes to the research plan

The COVID-19 pandemic had a significant impact upon the methodology and implementation of the research for this report: planned field visits to carry out in-person interviews and workshops became unviable and sources had newer, more urgent priorities than taking part in the research, causing delays and the need to change our methods.

However these inconveniences were minor when compared to the impacts upon the frontline community members and activists we were interviewing, many of whom not only experienced very high health related vulnerabilities, food shortages and communication difficulties, but also increased threats to land as state oversight diminished during lockdown periods. In addition, some reported increased surveillance of their activities with the introduction of regulations restricting their movement around territory, or through the introduction of virus or vaccine related apps which could track movement. There were also

reports that state officials took longer to respond to requests for help, citing delays caused by sickness and working from home, and police processes following arrests were slower, causing some people to remain in custody (under false or phony arrest charges)for longer periods.

There were also political changes across the regions where the research was conducted, with general elections and other political changes in many countries. The following are included as examples to demonstrate how rapidly changes can occur with far reaching implications for the security of environmental and human rights defenders.

Very significant for our research in Brazil was the election of President Lula da Silva and the leaving office of Jair Bolsinaro in late 2022. Under Bolsonaro the country saw escalating violence against Indigenous and other earth defenders and increased repression of civil society groups. It is hoped that their situation will improve given Lula's commitment to defending environmental rights, including the establishment of a new Indigenous People's Ministry and the appointment of Indigenous representatives in key positions.

Other dramatic changes in government have happened across the regions, including the military coup d'etat in Myanmar in 2021 which deposed democratically elected Aung San Suu Kyi and derailed the country's movement towards stability and democracy.

Similarly, the ousting of President Castillo in Peru in late 2022 has led to months of political instability and unrest and increased security concerns of frontline environmental and human rights activists.

Eight Discussion Themes

3: Discussion

The interviewees had a wide diversity of experience in using and interacting with technology as part of their land defense and human rights work, and had experienced a variety of different threats, however some common and overlapping themes emerged from our research:

1 **Personal safety and security**

2 **Digital tracking / surveillance**

3 **Risks of devices being stolen, seized, confiscated**

4 **General device and app security**

5 **Data security**

6 **Internet accessibility / connectivity**

7 **Technical literacy**

8 **Steps people are taking to protect themselves**

3.1 Personal safety and security

Environmental and human rights defenders worldwide face threats to their security, and these threats are particularly prevalent in countries run by oppressive regimes. Violence — including sexual and psychological violence — and other threats to individuals' safety are commonplace, and assassinations of earth defenders are increasing each year[2]. Interviewees in all the regions where research was undertaken reported at times fearing for their own, colleagues' or family members' safety, due to their work (Sources 2, 4, 6, 8, 12, 15, 17, 19, 18, 20, 21), and in all regions respondents reported collusion between state (including law enforcement) and company actors against them (Sources 2, 4, 5, 9, 15, 18).

The level and quantity of threats differed from place to place and context to context, some reported police violence against protestors (both within and outside of custody), destruction of land/property by government agencies, abuse of women in villages opposing extractive industries, being followed whilst working, and threats to life so serious that some individuals had gone into hiding or needed 24-hour protection (Sources 2, 4, 6, 7, 8, 9, 21).

The addition of technology into the mix raises new questions and more possible threats as individuals could be more exposed whilst collecting evidence, and therefore at risk, or they could be specifically targeted in order to retrieve / destroy the data. Source 7 knew of a community member who was chased down by members of a state agency, beaten and attacked for filming illegal activities, and the camera they held was destroyed. In another case reported by Source 4, shots were fired into the air by company employees in order to scatter a group collecting evidence about illegal land invasions, and the interviewee expressed fearing repercussions if evidence was found on their phone.

The relative security of individuals once data is made public was a question people felt differently about. Some sources (12, 15) felt like the threat to them as individuals decreased once evidence was published on a social media site or elsewhere, whereas one source reported that publishing on social media could make the individuals a target of state

[2] Global Witness 2021, Last Line of Defence, https://www.globalwitness.org/en/campaigns/environmental-activists/last-line-defence/

violence, and that some states had accused earth defenders of publishing 'fake news' when they did so, leading to arrest and prosecutions.

Interviewees acknowledged ambiguous feelings about whether data collectors should be identifiable within any apps used. On the one hand, respondents felt that this could be a risk if information fell into dangerous hands, as witnesses could be identified and targeted (Sources 2, 8, 11). On the other hand, some data administrators stated that being able to identify the data collector would help with their workflow and verification of data.

One danger which a few interviewees (Sources 2, 9, 17) mentioned was linked to judicial and legislative harassment, a technique used by the state — often in collusion with private actors — to criminalize activities of frontline earth defenders. Laws are created which target activities of land defense or enable legally sanctioned police responses to their work.

In one country the police need to be notified in advance of public demonstrations, in theory in order to provide protection to those demonstrating. However sources allege that this has resulted in heightened police violence against protestors and bogus arrests to intimidate human rights defenders (Source 9). It has also resulted in the police spreading misinformation to organizers, such as telling them that they now also need a permit for certain gatherings and meetings — which they don't — in order to track and infiltrate their activities (Source 2).

Threats to livelihoods were also commonly reported: Source 20 told how water was cut from their village after they objected to unconsulted expansion of an extractive industry onto their lands, and that elsewhere farming land was flooded with saline water and crops were destroyed after a conflict with a separate company.

Threats could also be incidental, depending more upon the location or environment worked within. Source 8 told how there are places they need to visit for their data collection which, if they were to enter them without informing the authorities and national park service, they could be shot on sight, as they would likely be taken for a poacher, who themselves are a security threat to the park rangers. In addition Source 1 told how certain areas of their

territory are off-limits for data collection due to the dangerous wildlife inhabiting there which potentially presented a risk to life.

Women respondents also mentioned receiving in-person and online harassment due to their gender, mentioning the fact that they are working in a predominantly male space, and there were reports of targetted sexual violence against female environmental and human rights defenders (12, 21).

3.2 Digital tracking / surveillance

Respondents in all areas where research was conducted reported cases of known or suspected digital surveillance of their or their colleagues' activities by company or state actors, with phone tapping being the most commonly reported, but also hacking of computers, tracking on social media and cloning of WhatsApp accounts (Sources 6, 9, 12, 15, 18). In some cases respondents mentioned that such surveillance had led to judicial harassment of some civil society organizations that advocated for environmental and human rights defenders (Sources 2, 5, 9, 18). In one case a national NGO was questioned by a government ministry about their use of Virtual Private Networks (VPNs), evidence that the state had been tracking this activity. In other cases respondents mentioned that NGOs had been forced to close following systematic harassment, or legislative changes which criminalized aspects of their work (Sources 5, 6, 2).

State agencies in South East Asia appeared the most organized in terms of surveillance, with people being arrested after posting about human rights abuses on social media and prosecutions of earth defenders for fake news.

There were fears that sophisticated surveillance technology from the Chinese Government was being used by strongman governments across the world, including in South East Asia, Africa and Brazil, with some respondents reporting being under observation from companies through drone surveillance (Sources 5, 18). The creation of a general culture of fear and peer surveillance, including peer informing and social media surveillance, was also reported – evidence of the range of tools oppressive states have at their disposal (Sources 5, 6, 18).

The prevalence of phone tapping caused many informants to report that they were learning to become more cautious about which apps they used for messaging with colleagues. For example, Source 12 said that after their meetings were continually interrupted or infiltrated by police or others, they no longer arranged meetings over the phone, or passed any important information that way, but focused on in-person meetings.

In Brazil respondents reported concern around using new digital tools, fearing that if they did so the surveillance of them, and associated risks, would increase.

3.3 Risks of devices being stolen, seized, confiscated

Confiscation or theft of phones, cameras or other equipment, was something that had happened in all the regions of research, and interviewees from each area had either experienced this themselves, or had colleagues who had experienced it. The fears surrounding such device loss were different, depending on what information was being collected and also the identity of those who seized the devices. In some cases it was the loss to the project of a valuable device and important data which was feared, in others it had more to do with data getting into hands of others who could use it for their own purposes and/or to target earth defenders further (Sources 6, 7, 18). The greatest fear related to devices and data getting into the hands of state departments with resources and technology to access data and track activities of device owners.

One way devices were taken, reported by a few individuals, was if they were arrested by the police, and sources 5 and 18 deemed this to be the main reason for arrests they had knowledge of (in order to confiscate the device and data). In some regions workers from companies extracting natural resources from community lands were also reported to have stolen phones where photos and other data were being recorded, and, in one case, phones and cameras were destroyed by agents suspected to have been hired by a company working in collusion with the police (Sources 4, 6).

When asked, interviewees reported that, in most cases, those holding the devices had very little time/capacity to do anything to devices prior to them being taken. In cases where

there was more time or opportunity, respondents reported throwing devices to others for safe keeping, or dropping a phone in a river in order to avoid it being taken (Sources 2, 4).

3.4 General device and app security

There was diverging experience and opinion about how to keep devices and data secure from third party access, due to a number of factors, such as who ordinarily had access to a device, the degree of technical literacy and the type of threats identified.

On the one hand, some interviewees responded that their phones were used by their whole family, and sometimes lent to friends, due to there not being many phones available in their community (Source 2, 8). In these cases they reported not using a password on the phone, in order to keep it available to others, however there was interest in having more security specifically on access to the applications used to collect evidence.

In another case, where the access to devices was more controlled, the phones were already secured with passwords, and unsecured devices were not be considered safe enough for storage of the sensitive information being collected (Source 6).

In general, there are contrasting views about what security measures are viable. Coordinators and advocates — who generally have greater technical literacy and are more used to handling sensitive digital data — were keen for high security, with password enabled apps and differing levels of access to data. On the other hand, community-level data collectors and earth defenders — who might use whatever devices they have at hand to collect the urgent information they need to provide evidence of environmental and human rights abuses — mentioned that for apps to be used with ease by populations with low technical literacy, they need to be very community friendly, work offline and have inbuilt, simple security which doesn't provide a barrier to use.

3.5 Data security

Data security was a concern for most respondents, although amongst most frontline users there was little knowledge or culture of practice for taking any precautions. There was

however enthusiasm expressed about learning some techniques to secure data, and for the potential for applications to automatically encrypt any data sent.

WhatsApp was the app most commonly cited by users across all research areas as being used to transfer information and make arrangements regarding environmental and human rights work. Knowledge about its level of security was varied, however even amongst those who spoke of mistrust of it due to its ownership, and concerns about privacy, expressed difficulty in shifting to platforms they deemed more secure. However some respondents reported that a recent increased understanding of the vulnerabilities in some messaging tools is leading them to use alternative methods when threats appear serious (Sources 2, 5, 8, 18). However, as not all those involved in the work have smartphones, some respondents mentioned that they either had to take a risk and transfer information via a simple text message or voice call, which they considered insecure, or try to meet together in person (Sources 9, 12).

The level of trust of colleagues and other team members is a significant factor in their consideration of how secure their data is. In many areas trust is the cornerstone of land defense methodologies: close-knit teams bound by culture, ties to land and often kinship. However in other areas such trust is almost totally absent. Data coordinators identified risks to data if team members switched allegiances, or risks to individuals if their identities were visible in apps. As one said “Loyalties are very fluid and that affects the perspectives on control within devices” (Source 5).

When asked about Mapeo specifically, one respondent said that they currently considered it to be a secure option for data collection as other local actors weren’t aware of it, and assumed they are just taking photos or looking at their phone, oblivious to Mapeo’s potential to collect information in an organized manner (Source 4).

An further risk to data comes from vulnerabilities within operating systems. Devices held in communities with low technical literacy and/or limited internet connectivity more likely be older devices and/or use out-of-date operating systems which are still open to security vulnerabilities addressed in newer systems (Source 18).

3.6 Internet accessibility / connectivity

Internet accessibility and connectivity was generally very low across all the regions and for all respondents, due to their tendency to live and work in remote areas, often with low population density and possibly with forest cover, mountains or other features which inhibited connectivity. This is itself a direct security concern if people encounter danger or threats and are unable to quickly communicate for help or support (Sources 1, 4). For most respondents this question was also relevant in terms of the ease with which they could send and receive information gathered on environmental or human rights abuses.

A total lack of phone signal in rural home and field environments was common for frontline respondents, although coordinators tended to live in more urbanized areas where connectivity was greater. For many users access to the internet was available in local towns, however in some cases travel is expensive and time consuming and either not available to all, or not possible on a frequent basis (Sources 4, 5, 6, 11).

Access to mobile data credit, even if there is internet available, is another factor, as users might not have any credit, or ability to buy credit (lack of resources or lack of local top up facilities). There might also be different networks available in different places, with some respondents having more than one phone or SIM in order to have greater connectivity possibilities (Sources 2, 15).

Unstable and unreliable connections were also common, sometimes being influenced by the weather conditions. In some areas connectivity could be found by standing in certain spots within villages, or climbing certain hills — but in such cases the individuals are out in the open and one respondent mentioned this as a security threat whilst sending data (Source 6). The unreliability of connections means that environmental and human rights defenders can not depend on being able to send alerts with evidence, or seek backup if they feel threatened themselves, even if they have devices and data credit.

Respondents in some areas reported that in some states in South East Asia and Sub Saharan Africa there were occasions when the Government restricted access to the internet, or to certain websites, in order to repress local communications and organizing efforts (Sources 1, 5). This was not reported as widespread or frequent, but communities

living in these areas felt it as a continuous potential threat which has been utilized in the past.

3.7 Technical literacy

Interviewees had a wide range of technical literacy: some people had only started using a smartphone within the last year, whereas others were university-trained technicians. However the majority were mid-level users, comfortable with using a smartphone and perhaps a laptop.

Respondents identified technical literacy being a challenge if their work depended on community members who had lower literacy levels being able to use apps to gather data. Some particular aspects identified repeatedly as being issues were:

- **Language**: language barriers in apps, either language literacy if community members were generally non-literate, or did not speak / read the app language, or the use of technical terminology which caused confusion or misunderstandings (Sources 5, 17). When looking at Mapeo designs the term passcode was one term reported as confusing by Sources 8 and 11.
- **Passwords**: there were diverse opinions about the usefulness of passwords for phones or apps. In one case it was seen as an essential feature for any app used by the land defense team, whereas in another case the coordinator considered that forgetting the password was a greater, and more likely, risk to data loss than a phone being taken by others (Source 7).

- **Ease of use of the app and workflows**: Where apps were being used by a large number of people within a project, having simple workflows, and a limited number of them, was deemed important to keep people on track with the essential data they needed to collect.
- **Security**: there were diverging views on which security aspects should be default or customizable within the device or tool. This tended to depend either on the technical literacy of users or levels of trust within the wider team (Sources 7, 20).

3.8 Steps people are taking to protect themselves

As the dangers to environmental and human rights defenders increase, so local and national earth defenders and their allies are taking steps to protect themselves and their work, be it from physical or online attacks, or threats to data. The interview respondents reported taking the following measures. Source referencing has been removed to increase anonymity.

Team practices

- Hiding the fact that they are collecting data by making it look like making a phone call, or hiding the phone behind a bag.
- Going in groups when doing land defense work to ensure there are witnesses and for added security.
- Trainings on personal security for the team including how to de-escalate situations of conflict.
- Traveling to higher-risk areas by secret / roundabout routes which are less observed and will not bring them to the attention of company / state agents.
- Hiding phones when not in use.
- Approaching international organizations and special rapporteurs to spotlight issues and for emergency support.
- Developing a security protocol about data collection and storage.
- Implementing a digital alert system for high-risk people and scenarios. One source reported teams using a personal GIS alarm system.

- Meeting in-person when possible, avoiding sharing information over phone / messages.
- Bullet-proof vests and bodyguards in cases where physical security was seriously threatened.
- Doing a ceremony to ask the ancestors for spiritual protection for the team before undertaking any dangerous work: “The protector has to be spiritually protected before they can protect anyone else or their land”.
- Going into hiding if threats to personal safety are deemed serious.

Digital / device related practices

- Using a pseudonym on devices to protect identity in case of device seizure or hacking.
- Turning phones off when not in use to avoid some tracking mechanisms, or using multiple phones to this same end.
- Collecting evidence on more than one device or sharing any evidence immediately with others so that there was less danger of evidence being lost.
- Using a secure and encrypted messaging system between team members.
- Backing up data to a shared cloud-based account.
- Creating a protocol including a digital workflow which is customized to the particular apps used.
- Closing any data collection apps after use.
- Using the TOR browser to protect web anonymity.

4: Conclusions

The research discussed above contains many overlaps in terms of felt and perceived threats and responses from our interviewees, but also a diversity of experience and need. It is clear that there is no one-size-fits-all solution. Security protocols, behaviors and advice needs to be tailored to particular local circumstances, and updated as local or national conditions change.

The majority of the threats reported by interviewees relate to physical threats to their security, often whilst they are in a data collection situation: for example documenting illegal activities. Technologists, understandably perhaps, tend to see things through the lens of tech and look for tech-based solutions. However, at the point at which an individual is threatened with violence and forced to reveal the data they are collecting — opening apps and inputting passcodes — there is little that can be done to protect data from being seen[3]. Of greater importance will be the protocols they have developed as an individual or team to safeguard against this opportunity arising.

Security within technology generally becomes more important either if it can replace the need to enter a dangerous situation — such as documenting from afar — or once data is collected and is being stored, shared or made public. The challenge for technologists, including the Digital Democracy Team building Mapeo, is to keep tools flexible and adaptable, and to balance security measures, so as to lock out actors with malign intent, whilst ensuring data owners can still use the tool and access data with ease.

The following summarize some of the differing and occasionally contradictory needs that users have, as reported by our interviewees, and how these translate into challenges faced by designers of locally led technology attempting to keep data and users secure.

- **The importance of general tech security knowledge:** people use a range of apps for communicating and sharing data with colleagues. Therefore even if the main

[3] The Dd team is exploring options to hide data (using sealed box encryption) and decoy apps which might be helpful in some such circumstances. The ability to see identities of people involved in a project, as well as ability to edit data, are other security risks which need to be considered in cases of device seizure, which could be protected against.

apps used for collecting and storing evidence have high security, users need to be aware of vulnerabilities within any apps they use to share it externally.

- **Ensuring data is useful:** For data to be useful, it generally needs to be shared. Developers need to find a balance between keeping data private and secure until/if the user wants to share it with others.
- **Anonymity or identification:** The balance between protecting users' anonymity within applications, to prevent them being identified if devices are hacked, versus the need some projects have to trace those who collected certain data, to support evidence-based verification processes.
- **Passwords and access:** The risk of losing access to data due to forgetting a password might in some cases be higher than the risk of data being compromised in other ways if a password is not used.
- **Ease-of-use:** The tension between having easy-to-use, convenient tools, and ensuring security measures are high enough. If a tool is not easy enough to use there are risks people will switch to using a less secure, but simpler app.
- **Low tech literacy and trust in the technologists:** For example encryption of data and online storage: if an app claims that data is encrypted what does this mean to people with low tech literacy; how can developers ensure that users with low tech literacy are properly informed in their decision making.
- **Trust within a team:** Different social structures or levels of trust between teams or data collectors can be diverse. In some systems everyone trusts each other, in others there might be mistrust, changing alliances or a need for differential access, and these will influence feelings around anonymity and sharing of data.
- **Online versus offline**: Having data backed-up online can secure against its loss and can reduce the need for risky in-person meetups. However, partially or totally online systems expose data and individuals to insecurities if the Government or others can hack into them, or if access to the internet is difficult, unreliable or vulnerable to state shutdown.

The Digital Democracy Team is taking all of the findings of this report into consideration as it continues both the design and development process of Mapeo, and accompaniment work

with local groups. A number of new security features have already been designed for Mapeo which build from needs and views expressed by interviewees and reported here, which we will be releasing later in 2023.

We also hope that this report, and the invaluable views and experiences of our interviewees, will be of use to technologists around the world working on similar themes.

> "There is no one set of solutions that can resolve all the needs of land defenders, but clarifying which needs are the priorities of the communities that the technology is in service of, is a good reference point for the compromises that inevitably are made when designing for the most vulnerable technology users." Jen Castro, Codirector Digital Democracy.

Digital Democracy

Thank You

Visit digital-democracy.org to learn more.

Report compiled by Aliya Ryan, based on research carried out by the Digital Democracy Team

Research made possible by support from Open Technology Fund

www.digital-democracy.org