Ethical Guidelines

for PeaceTech

JUSTPEACE Labs

Ethical Guidelines for PeaceTech

Published by:

JustPeace Labs
Justpeacelabs.org
@justpeacelabs

For more information contact:

Jennifer Easterday
CEO & Co-Founder
jen@justpeacelabs.org

Contents

Introduction

More and more peacebuilders are turning to technology to help their work. At the same time, some of the world's largest Internet and Communications Technologies (ICT) companies are entering the market in post-conflict countries. These developments raise wide-reaching ethical considerations and concerns regarding users' privacy and security.

A number of preeminent organizations and scholars in the field have already acknowledged the challenges posed by the growth of the global tech industry, particularly as concerns the rights of the world's most vulnerable citizens. In picking up where they have left off, we propose a set of ethical guidelines for PeaceTech practitioners engaged in conflict or post-conflict markets. It is meant to be a practical tool that provides guidance on questions and issues to consider, as well as valuable resources for diving deeper into particular issues.

Given this objective, the Guide focuses exclusively on (i) ethical and security considerations related to (ii) the use of ICT in (iii) recently post-conflict countries. Although the challenges discussed herein undoubtedly exist in developed country contexts and at times of peace as well as conflict, the uniquely sensitive nature of recently post-conflict countries exacerbates these challenges and therefore presents a need for heightened caution.

The Guide is loosely organized by a program or project lifecycle. The first section introduces ethical, privacy and security challenges and includes a discussion of the types of harm and ethical considerations that arise when using ICT in peacebuilding or post-conflict contexts. The second section presents considerations for how to meet ethical obligations in practice, from the planning and strategy phase onward.

Understanding Ethics, Privacy & Security

Protecting Users

There are many risks associated with using ICT in post-conflict contexts, for both users and organizations. These include the risk of physical harm, shaming, retribution and group harms.

Risks and harms may change over time, as situations become more stable or more violent. Risks can also evolve as the result of the technology project itself. Participating in technology programs, using technology or downloading/possessing a mobile application can create a greater risk of physical security threats or retribution for users.

According to the International Committee for the Red Cross (ICRC), using technology in post-conflict settings brings unique challenges. These include, in order of importance:

- *"The protection of [users] unaware of the risks of being identified or tracked by the authorities or armed groups who might take actions against them. In some cases, retaliation might affect a whole community."*
- *"The loss of control by users over their personal data. Once their data has been made public on the web, it is nearly impossible for users to reclaim, modify or delete the data."*
- *"The misuse of personal data. This can happen with ill-intentioned people and private organizations wanting to take advantage of the vulnerability of people to gain financial advantages, or to sell their services."*
- *"The risk of raising false expectations that there will be a rapid response or in fact any response at all to the concerns expressed by individuals or communities."*
- *"The inability of people who have had little or no exposure to or experience with modern information technology to give real informed consent (for example to local activists putting online stories they just heard in the street)."*
- *"The reliability/distortion of information due to bias or danger of manipulation such as:*
  - *the difficulty of identifying the first source of information and the authenticity of this source;*
  - *the bias due to unequal access to technologies in different regions, or across generations;*
  - *the bias aggravated by Internet viral loops that might favor certain information and sources to the detriment of others;*
  - *the purposeful manipulation of information by those with vested interests."*
- *"The risk of favoring one-way communication from individuals to protection organizations coupled with mass communication from protection organizations to individuals, versus a more in-depth dialogue (since the capacity of individuals to send messages by far exceeds the capacity of organizations to respond to them individually)."*
- *"The diminishing incentive for individuals to resort to more traditional face-to-face interviews with humanitarian and human rights workers, when they would in fact have the possibility of doing so."*
- *"The pressure on organizations to communicate publicly and rapidly."*
- *"The information overload."*

(ICRC, 82 – 83)

Understanding Context

In order to properly understand the context of the program or project, conduct a Conflict Sensitivity Analysis (CSA) and/or a Peace and Conflict Impact Assessment (PCIA). Ensuring a deep understanding of the context in which the program or project is deployed throughout the organization, from field staff to software engineers to executive management, is critical to effectively balancing risks and benefits. There are many guides for CSAs and PCIAs available, some of which are listed in the resources section.

- Communicate and engage with the communities in which the project will be deployed.
- Engage with local organizations, experts and the sources or end-users to develop an inclusive understanding of risk, local context, local policies, etc.
- Consider the regulatory environment, including policies, laws and other rules that may impact how tech-supported projects are owned and can operate.
- Consider the political environment, including how changes in political parties could change personnel, structure and/or mandates of government ministries.

> *"Data-driven interventions may be met with suspicion in locations impacted by colonial oppression, repressive State surveillance, or mistrust of foreign corporations. The very introduction of data-centered technologies can both reveal and exacerbate power relations and asymmetries such as mapping tools that could unexpectedly make political affiliations visible."* (Latonero and Gold, 9)

- Understand existing power dynamics and how the project may reproduce or amplify structural conditions such as racism, gender discrimination, power imbalance, disempowerment or inequalities.
- Consider rights of and risks to individuals as well as groups (such as women, children, the elderly) and communities.
- Understand how the project may create vulnerabilities for certain populations or communities.
- Plan and budget for CSAs and PCIAs. Properly conducting these assessments will likely require additional time, costs and potentially additional staff who have the required expertise. Re-evaluate and update the assessments as the situation changes and at every stage of the project.
- Consider the level of literacy of your users and plan to use pictograms or other forms of communication as necessary.
- Consider the language requirements of your users and plan for the ability to have your technology available in relevant languages.

Ethical Obligations

Your seven ethical obligations are:

- **Respect**
- **Do no Harm**
- **Non-Discrimination**
- **Informed Consent**
- **Privacy**
- **Security**
- **Data Ownership**

Respect

Respect for the individuals and communities who use or benefit from your technology project should inform every decision you make.

- Regard every person as autonomous and free to make his or her own choices.
- Give every person the information needed to decide whether or not to participate voluntarily in your project and the right to easily access, correct or remove their data.
- Develop an understanding of cultural norms (see Understanding Context, above).
- Treat users as equal participants in the project, not as victims or beneficiaries.
- Understand and consider any power differentials between you and your users and strive to develop a balance of power by involving the user and their community in the design and evaluation of the project.

Do no Harm

"Do no harm" is a foundational ethics concept. In practice, it involves a balancing test: your involvement in this context must always must do greater good than harm.

- Conduct a risks/mitigation analysis at the start of a project—identify and rank (high, medium, low) all potential risks for users and your organization and identify steps to mitigate them.
- Consider the following questions about the data you collect from/about your users:
  - *Could the data be used for military or police intelligence gathering?*
  - *Could the data be used by any ill-meaning third party?*
  - *Can the authorities trace the information back to its original source?*
  - *Are the channels used to convey data secure enough to transmit personal or sensitive data?*
  - *Are you capable of securing the data against the risks identified in the risks/mitigation analysis?*
- Consider risks to the organization itself, including risks to its ability to gain and maintain access to users.
- Plan for the end of the project and ensure that data does not get left on an outdated or insecure system.

Non-Discrimination

The project should take a non-discriminatory approach and also strive to avoid creating or replicating discriminatory structures. Non-discrimination may arise when deciding which user groups to target and who to exclude.

- Understand how the use of technology or data can have a discriminatory effect in your project's specific context.
- Consider whether there is unequal access to technology amongst users (such as in different regions,

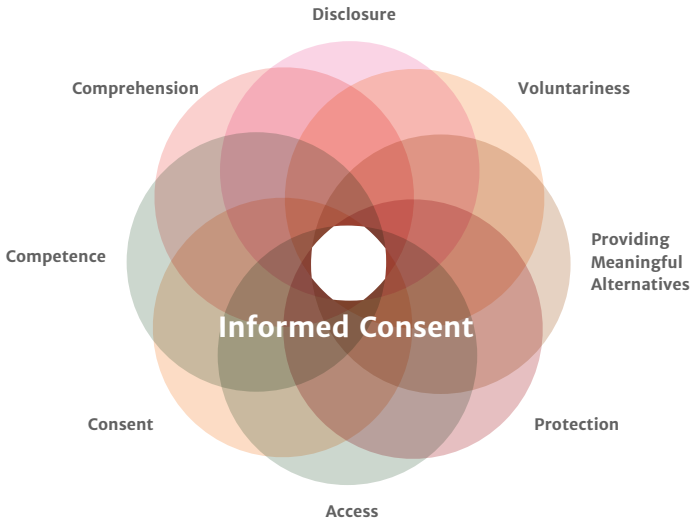
across generations or between genders) and whether this creates a bias in the collection of information or use of technology.

- Consider whether your target user group has been selected because of their accessibility, language ability, educational level or position in society, to the exclusion of others. Attempt to remedy any exclusions.

Informed Consent

Informed consent is one of the most challenging ethical obligations to get right, especially when working with low-literacy or vulnerable populations. It is imperative to communicate—in a simple, easy to understand and culturally relevant way—the purpose of your project, the risks participation entails and what you will do with any information gathered through the project.

Informed consent is based on competence, comprehension, disclosure, voluntariness, providing meaningful alternatives, protection, access and consent. These same principles apply for other types of user agreements and terms and conditions.



- **Competence:** Ensure the user is able to fully understand the implications of participation. Determine whether the user needs a special consideration (e.g., children, persons with a mental disability, survivors of recent trauma and violence). Consider options for obtaining consent from a legal guardian—do not proceed if you are unsure of their comprehension of the implications and potential risks.

- **Comprehension:** Ensure that the user understands the implications of participating and providing data/information. This may be difficult if the person has a limited understanding of ICT or the Internet. Find a balance where the technology is explained clearly, simply and respectfully and in a way that protects the person's safety.

- **Disclosure:** Introduce the technology and organization. Describe the technology and how you plan to use the data, including under what circumstances you may be legally required to release the data to authorities.

- **Voluntariness:** Ask for permission to use the user's data and whether they are willing to be identified by name. Ensure the user is participating voluntarily and that they clearly understand the purpose of the project, implications of participation, how the data will be used, who may access it and where it is stored.

- **Meaningful alternatives:** People can be overwhelmed by information. Even where people understand, sometimes consent is not a choice unless there are meaningful alternatives—so provide meaningful alternatives.

- **Protection:** Ask if they want their identity protected. Explain the available anonymizing methods and the implications of using it.

- **Access:** Be clear about who has access to the data, for what purposes and under what circumstances. Also include information about any potential transfer of the data to third parties, whether part of a current or future plan, and what related security measures have been taken.

- **Consent:** Forms designed to obtain informed consent should include:
  - *Name/Username and/or identifying criteria (address, email, phone number)*
  - *Clear statement of intent covering the purpose of the information sought and the intended "scope of use"*
  - *Specific statement of consent to handling his or her personal information and conditions under which information may be shared (including identifying individual by name, voice or face)*
  - *Itemized agreement specifying how you may use the data (collection, storing, changing, processing, reproducing, distributing, sharing with third parties etc.)*
  - *The user should be made aware of and consent to distribution via the Internet, including the understanding that content may be viewed and used by third parties (including the authorities, courts and others)*
  - *Time-frame for which the consent is valid (once this period is over, you are required to either get another consent agreement or destroy the data)*
  - *Specific clause enabling the user to rescind permissions at any time*
  - *Date of agreement*
  - *Contact information so that the participant can reach you*
  - *Details on how long the information will be used/kept and how and where it will be stored*
  - *Reminders that the user can cease participating at any time and request that their information be destroyed, whenever feasible.*

WITNESS includes the following questions when obtaining informed consent:

"Do you understand what we are doing?"

"Do you consent to your data/information being included in this project, including video and any other forms of media that may be used (print, photos, website)?"

"Do you know who may see or access the information?"

"Are there any restrictions to using the data/information you provide us with that we need to be aware of?"

- Use simple terms and appropriate language(s). Consider options for users with no or low literacy and various language requirements.
- Ensure the informed consent information and request is provided in ways that are culturally appropriate and relevant. Consider asking users to explain in their own words what they are consenting to, to provide an accurate reflection of their understanding of their consent.
- Informed consent information should be kept securely and ideally in a way so that if the data is confiscated or otherwise accessed by an unauthorized person, the identifying information about the user and their network is kept secure.
- When using a website, the website should be transparent and explain:
  - *The identity of the project organizer(s)*
  - *The purpose of the website/project*
  - *How information gathered via the website will be used or processed*
  - *Who the information may be shared with*
  - *Who can access the information*

- *How personal data can be modified or deleted if necessary*
- *The protection measures used by the website itself, such as HTTPS, no use of advertisers or cookies, etc.*
- *The potential risks of sharing information and how to mitigate them (anonymizing, secure passwords, disabling geo-location identifiers, etc.). Consider offering secure alternatives to accessing the website, such as a GlobalLeaks deployment, SecureDrop, TOR .onion site or similar.*

- When collecting informed consent from individuals is not possible, conduct assessments such as:
  - *A "professional practice" assessment based on objective, established principles and professional practice; or*
  - *A "reasonable person" test carried out by a well-informed person who attempts to establish what a user might be expected to grant.*
  - *Decisions should then be made based on an assessment of users' best interests, in consultation with relatives, a legal representative, caregivers or others close to them.*
- Details of users' consent should accompany the data throughout the data cycle.
- If consent has not been given, is missing or has been restricted in any way, the data should not be transferred to a third party.
- Obtain additional consent if the data is to be handed over to a third-party or used in a way not previously disclosed. Exceptions to this apply when the protection of vital interests of the person concerned, or of others, is at stake.
- Consider relevant laws, including data protection laws, international human rights and international humanitarian laws.

> *"Having obtained the necessary informed consent does not remove the actor's responsibility to assess the risk, for an individual or a given group, of collecting, storing or using sensitive information. If the risk is seen as too high, or as liable to increase over time, information should not be used, even if informed consent was obtained."* (ICRC, 94)

Privacy

Protecting personal data is based on the right to privacy recognized in most general international human rights treaties. Privacy is distinct from security. It relates to how we control access to personal information/data and the extent, circumstances and effects of sharing that information. Even if information is anonymized or aggregated, it can lead to the identification of individuals.

- Develop privacy policies that govern the use of technology and data in your project, program and/or organization, using existing industry standards as a guide. Relevant standards are included in the Resources section.
- Conduct Privacy Information Assessments (PIAs) for each project. Examples of how to do this are included in the Resources section.
- Budget for ongoing privacy protection and support. This includes funding for PIAs and regular reviews of privacy policies and processes to ensure they are working and are up to date.
- Adopt the principle of minimization—only collect essential data, keep it for the minimum possible time and destroy the data when no longer needed. Be aware that this principle might not align with the interests of others (partners, stakeholders etc.).
- Anonymize by default. Consider the context and needs for privacy of personally identifiable information when designing solutions and mitigate accordingly.

The default should be to only collect anonymous information; only collect personally identifiable information if it is critical to your project.

- Consider using a logging system for sensitive data where the system logs who accesses the data at all times.
- Be aware that anonymizing data in order to protect privacy can reduce the data's utility. Plan for this and adopt strategies to mitigate.
- Be transparent, always. Design transparent policies that describe data processing flows at the start of the project.
- Assign a person to oversee privacy matters, including discussing your privacy policies with users and answering their questions. Make that person visible and widely available to discuss privacy with users.
- Be accountable, always. Create internal governance structures that deal with accountability and enforcement for breaches of privacy and related problems, including notification for victims of a breach.

> ***"Some basic principles of privacy:*** *Be proactive, not reactive; treat protection of personal data as a default setting; embed privacy into design; offer end-to-end security for personal data; be transparent about how data is collected and used; be responsive to concerns and queries; ensure data accuracy and confidentiality."* (ICTD Principle 8)

- Provide easy to understand privacy resources and guidance for staff and contractors.
- Know the privacy capabilities and data use policies of all technologies (including partners' platforms, cloud-based services, messaging services, etc.) used in the project.
- Know the law and policy about privacy and data protection in your jurisdiction(s), but be aware that the international regulatory landscape regarding data privacy is fragmented and may lack adequate accountability and enforcement mechanisms.
- Domestic or regional laws might require disclosure of confidential data, based on public safety and rule of law concerns (such as in criminal cases). Develop and follow clear internal policies and guidelines defining the circumstances in which such information will be shared and disclose any requests for disclosure to the relevant user.
- Domestic or regional laws might also prohibit encryption in some data communications, which may impact privacy and security procedures.
- Failing to learn the law could prevent data collection, technology use, require data disclosure or bring about legal action by the State or individuals concerned.
- Make it easy for users to make informed decisions about their privacy.
- "Privacy" should be the default setting. Do not ask users to activate privacy settings or ask them to "opt-in" to privacy or "opt-out" of non-privacy standards.
- Ensure users can simply access, correct and remove information they have previously uploaded or shared, either through the software or by contacting an administrator.
- Ensure that users can make decisions about whether and how third parties collect, access and use their information.
- Networked data can reveal relationships and characteristics about others without their knowledge, including individuals who are not directly participating in the project. Be aware of this in safety and privacy assessments as well as in data analysis.
- Consider allowing users to use a multi-factor authentication system for accessing their accounts.

- Incorporate automatic log-outs after a period of time and make active log-outs easy.
- If a user changes privacy settings to more public ones, make sure they are well informed of the potential consequences or implications.
- Disable location data settings whenever possible.
- Make it easy for users to delete their accounts.
- Establish a secure system for managing lost passwords or log-ins.
- Regularly update individuals with notice about how and when their data is being used, how and with whom it is being shared and who has requested it.

Security

Security concerns the disclosure of sensitive information or data to third parties, including through loss, theft, unauthorized access, disclosure, copying, use or modification. It is related to but distinct from privacy. Security when using technology for peacebuilding and in post-conflict situations also means protecting users from physical, emotional and other types of harms that arise when data is accessed by third parties or as a result of using your project's technology. Usability is a critical form of security—users can become discouraged or confused by overly complicated security measures or privacy settings. Tools need to find the right balance.

- Assess and mitigate risks to the security of users and their data. Balance the benefit of using data with the risk it entails to users and their communities.
- Conduct data security assessments for each project. Examples of how to do this are included in the Resources section.
- Consider whether sensitive information could be leaked or stolen.
- Understand the context of the situation in which you are collecting or storing data and whether there are any particular risk factors related to data security.
- Develop security safeguards that are appropriate to the sensitivity of the data collected before collecting any data.
- Assign a person to oversee security matters as part of their job role and responsibilities, including discussing your security policies with users and answering their questions. Make that person visible and widely available to discuss privacy with users.
- Clearly define tasks and responsibilities among staff, including defining supervision of data handling and the rights of individuals' access to sensitive data. This increases the accountability and security of the process.
- Be accountable, always. Create internal governance structures that deal with accountability and enforcement for breaches of security and related problems.
- Provide easy to understand security resources, training and guidance for staff and contractors.
- Ensure that staff of all levels understand that new technologies are highly susceptible and vulnerable to security breaches.

> *"Immediately putting online images of wounded protesters treated on the spot by volunteers can allow them to be identified with possible adverse consequences. Putting SMS or Twitter content online in real time revealing, for instance, the location of a women's refuge that was previously kept discreet might attract unwanted attention."* (ICRC, 86 – 87)

- As necessary, engage professional or expert advice from information management specialists when setting up data collection or transmission procedures.

Ultimately, this professional capacity should be built into the organization.

- Budget for ongoing security protection and support. This includes funding for data security assessments, penetration testing and regular reviews of security policies and processes to ensure they are working and are up to date.

- Assess relevant national legislation and practices on information protection and access to information. This can help you determine if it is necessary to refuse disclosing data to the authorities if requested to do so.

- Networked data can reveal relationships and characteristics about others without their knowledge, including individuals who are not directly participating in the project. Be aware of this in safety and privacy assessments as well as in data analysis.

- Evaluate risks that might arise from transmitting information, including to potentially malicious authorities or to organizations who do not have appropriate data security measures in place. This includes disseminating data through advocacy reports or the Internet.

- Where third party transfers of information are necessary, require them to sign a non-disclosure agreement and a strict data protection policy—and test it to ensure they are capable of protecting the data to the agreed standards.

- Consider whether sensitive information could be seized by an authority, either from you or other entities in the data processing cycle (such as mobile phone companies). Authorities might require the disclosure of data, for example for use in court proceedings. Users may not have given informed consent for this data use. It may also cause other unintended risks.

- Consider that using some technologies, such as short-codes and SMS, often means that any information shared over mobile telecommunication challenges may be accessed by or shared with other parties, including government agencies, marketing companies and data aggregators.

- Ensure that a full risk analysis is done before initiating contact through SMS or an app—be certain that no harm can come from such communication (such as an SMS), such as by having the message intercepted or read by the wrong person, including friends or family members who may not be aware that the individual had participated in the project.

- Treat information collected, especially if related to marginalized communities, as potentially valuable to adversaries, known and unknown. Generating data about individuals' identities, behaviors, activities and locations creates unintended outcomes and risks.

- Treat information collected about communities, including locations, activities, resources, needs, environment and economic activity, as potentially valuable to adversaries, known and unknown.

- Know all of the organizations that will handle data apart from your own, including sub-contractors, and their data security policies. Ask them to sign non-disclosure agreements stating that they have read and signed-off on all of your information security policies and protocols.

- Consider the security of transferring data, especially across international borders and including in the sub-contracting and outsourcing of data.

- Follow the suggestions in the Software Engineering & Design section, below. That includes practices such as:
  - *An initial configuration that by default provides maximum security*
  - *Security testing throughout the project and data lifecycle*
  - *Requiring strong passwords*

  - *Always having an updated system.*
  - *Regularly evaluate and update the security of the system*

- Adopt these practices when using or replicating sensitive data found online, through public websites, blogs or social networks. You are equally accountable for the risks and consequences of using this data.

- Adopt these practices when subcontracting information collection to others. It remains your responsibility to ensure that your partners apply the same standards and guidelines on the professional handling of information that concerns individuals or incidents.

Data Ownership

- Consider the data ownership rights of your users. When using or developing a platform where data is traded in exchange for free services (such as access to the Internet), weigh the benefits and risks of requiring users to provide personal information. This is especially true when working in regions with a history of instability or violence.

Meeting Ethical Obligations in Practice

Planning & Strategy

- Establish clear objectives and timeframes before starting a technology project or collecting data. Make sure that everyone on the team, from software engineers to marketing and communications staff, understand these objectives.
- Establish formal procedures for handling data, including collecting, compartmentalization, minimum access, auditing of controls and permissions, disseminating, storing and destroying data. This helps ensure that data processes are handled systematically, securely and professionally.
- Integrate data about informed consent, privacy, data transmission and restricted access into data handling procedures.
- Include information about data ownership, rights or deletion/correction and secure storage in data handling procedures.
- Review local, national, regional and international laws that are applicable (such as child protection, marketing and advertising, research, age, content, blasphemy, libel, use of images, encryption etc.).
- Conduct a risk assessment to help document the project design, decision making processes and indicate responsibility for different areas.
- Create a plan for how data will be destroyed or transferred to a trusted partner if or when the project ends or the platform closes down. Inform users of this plan.
- Develop a crisis plan with clearly assigned responsibilities to handle any conflict, privacy or security risk that develops.

Software Engineering & Design

The guidelines below are indicative of the approach that should be taken by software engineers and designers. However, it is not a complete guide to ICT privacy and security; industry standards, such as those developed by the International Organization for Standardization, should be followed as well.

- Technologists should seek outside expertise to help them understand the ethics and responsibility of applying technology in areas where they lack proficiency. This includes taking steps to understand the context, as described above.
- Consider implementing ethical safeguards into the technology and/or code itself, including through context-appropriate user agreements and privacy controls.
- Anonymize data by default. Only collect personally identifiable information if critical to your project.
- Avoid bias in algorithms.
- Future-proof your software to the extent possible, especially for security, privacy and data archiving.
- Employ minimum web security standards and proper procedural and technical controls to monitor unauthorized users and those that exceed their authorization.
- Before going live, test the security of any technology or website, including penetration testing and code auditing, if relevant. Consider publically publishing the results of these tests for more transparency.
- Plan and budget for ongoing security testing and updates.
- Use SSL, authentication and implement security features from the start of any technology project/program.
- Use Privacy Enhanced Technologies as appropriate.
- Encrypt data to 256 level if possible, or to 128 level at a minimum.
- Consider remote wiping options.
- Require strong password protection and auto-locking features.
- Ensure minimum privileged accounts, where users have minimal permissions and a role limited to the user's domain so that they cannot modify anything other than their own content.
- Validate all user inputs to avoid hacks.
- Secure data on encrypted channels.
- Establish 3-step force authentication.
- Establish regular secure data backups and store data in two separate places.
- Ensure that all data is password protected and encrypted throughout the data lifecycle, from collection through to storage and analysis to disposal.
- Avoid storing data on users' phones, USBs or flash drives in situations where these could be stolen or seized by authorities or others.
- Ensure that programs or apps are available in local languages and in formats adapted to those with low literacy, as necessary.

Providing Technology

- Consider the ethical and security risks associated with distributing technology, whether hardware or software.

> ***Ask:*** Will having an app downloaded generate risks for a user? Will carrying a particular piece of hardware (such as a smartphone) increase a user's risk for physical harm or theft?

- Where possible, utilize the transparency and security of open source technologies.
- Provide sufficient training on the use and security of any devices provided to users.
- Obtain your hardware (such as phones) from ethical sources, if possible. See the resources section for ideas on how to do this.
- Consider how to address any additional costs to the user, such as data, top-up credit, SIM cards, charging the battery or repairs.

Setting Expectations

- Set expectations and be transparent about the use and impact of the information provided by users and their engagement with the technology. To do this, you must understand the context.

Example: Providing technology for reporting human rights abuses could set the expectation that such abuses will be tried in a national or international court or other accountability mechanism. If such prosecutions are not forthcoming, users could become disillusioned with or distrustful of the project.

- Take action to mitigate any negative repercussions from mismanaged expectations.
- Create a dialogue. Two-way communication can increase trust, improve the quality and quantity of data gathered and inform privacy and security risk assessments.
- Keep users and communities informed of what is being done with the data provided, whether through an app, in person, town hall meetings, the radio, TV, SMS updates or another context-appropriate medium.
- As appropriate, update any websites or provide notifications through apps to inform users of how the information they have provided has been used.

Gathering Data

- Follow the suggestions provided above in the sections on Informed Consent, Privacy and Security.
- Set the scope of data collection based on the clearly defined operational objectives for the project (providing, operating or maintaining an application; meeting a business/program purpose the users are informed about; legal obligations etc.).
- Keep in mind long-term strategies and objectives and take advantage of the opportunity to collect information from users who may be difficult or impossible to reach later. However, in defining the scope of data collection, assess the benefits and risks of collecting sensitive information and whether it is necessary for your objectives. Collecting unnecessary information can cause preventable risks or set false expectations among users.
- Justify the need for each piece of data and personal information collected.
- Do not collect unnecessary data or data that can put users at risk of serious harm. See the Privacy section above for a discussion on the principle of minimization.
- Review informed consent (see above) before collecting data and ensure users have given active consent for the data you will collect. This includes:
  - *Making users aware of the time period for which their consent is valid*
  - *Making it clear to users how they can manage their consent*
  - *Informing users of any consequences of withdrawing or withholding consent and*
  - *Ensuring that users can easily withdraw consent without any undue delay or cost.*

- Review any security risks and be confident that gathering data is not exposing users to any unnecessary risk or potential threats or danger.

- Establish different levels of access to personal information and data based on the sensitivity and potential risks associated with the data. Match the different levels to traffic light colors (red, yellow and green) and ensure that each level matches a corresponding security protocol, encryption level, etc.

High risk: sensitive and private or confidential data requiring privacy and security protections; where confidentiality is required by law, policy or contractual obligations; where special authorization is required for use and collection; any personally identifiable information or data, including written, audio/verbal or visual data such as recordings, videos and photos.

Medium risk: non-confidential internal data that should not be publically shared; where unauthorized disclosure could cause material loss to the organization or brand, including aggregated data.

Low risk: public data that is not private or confidential and which does not invite any risk to users and whose publication would cause no adverse effects.

- Train users to disable Wi-Fi, cellular data signals and GPS when they are gathering or sending data unless a proper risk analysis and mitigation process has been conducted.

- Be aware that some users might be excluded due to language ability, literacy, political affiliation, educational level, access to ICT or the Internet or other factors. Take reasonable measures to avoid or minimize any biases that might result in unintentional discrimination or inaccurate interpretation of data.

- Write any questions or prompts in a way that avoids re-traumatization and is sensitive to the needs of users and their communities, including the level of literacy, language or whether they have experienced trauma.

- Write any questions or prompts in a context-appropriate way that avoids bias, discrimination or re-enforcing local power dynamics.

- Be sensitive to gender, ethnicity, religion, political affiliation, sexual conduct and sexual orientation when writing content, designing technology or collecting related data.

- Be prepared to provide information on appropriate service providers as referrals if members of an affected community or users seek advice and support.

Storing, Transmitting & Managing Data

- Follow technical measures and good business practice to ensure that data is transmitted, stored and managed in a secure and safe way. This includes:
  - *Ensuring apps and software are password protected*
  - *Encrypting data*
  - *Anonymizing large data sets as early in the process as possible*
  - *Transmitting data on encrypted channels*
  - *Setting data retention and deletion protocols and*
  - *Destroying data when no longer needed.*
- Take steps to ensure that unique identifiers apply only to one user to avoid potential privacy implications (such as if a mobile phone or SIM card changes hands).
- Assess whether authentication is required and apply it as needed/when possible.
- Anonymize data that will be kept for longer periods, shared or which could put users at risk.
- Protect chain of custody as necessary through a logging system that tracks who has accessed data, when it was accessed and whether it was manipulated in any way.
- If the data is very sensitive (e.g., health information, violence-related etc.), consider installing a secure local server or other mechanism to ensure that data is not stored longer than necessary and is stored and transmitted securely. If the local server connects to or touches the Internet in any way, it should be carefully managed by capable staff to ensure it is protected, updated, secure, etc.
- Conduct regular reviews of privacy and security protocols and assessments before transmitting or disseminating any data. Even if informed consent was obtained, circumstances may have changed that could cause an individual to rescind that consent.

Analyzing Data

- Understand and mitigate social biases and assumptions in data. "Bias" is any systematic distortion of information, whether or not it is intentional. Bias can come from the person collecting information or the person providing information.

Bias factors include:

- Limited coverage
- When the information collector is able to access all or a representative sample of information
- Communication barriers
- Prejudice
- Unequal access to devices, mobile phone networks or the Internet
- An information provider's inability to recall events
- False or exaggerated reporting from information providers due to social pressure, political or ideological convictions, or attempts to influence the provision of aid or assistance.

- Be transparent about the limitations in your methodology and results when analyzing and disseminating data.
- Be aware of the context—who has access to technology, the biases of self-reporting, any relevant ethnic tensions—and build this into your analysis.
- Networked data can reveal relationships and characteristics about others without their knowledge, including individuals who are not directly participating in the project. Be aware of this in safety and privacy assessments as well as in data analysis.
- Be aware that data can reveal false positives and false negatives. Try to control for this and be transparent

about it. Actions may be taken based on inaccurate data, models and predictions that can have unforeseen negative consequences for affected communities, sources and users.

- Be aware of and try to mitigate the risk of manipulated or exaggerated data reporting from users.
- A combination of methodologies and sources (for example, crowdsourcing and aerial imagery) can help minimize the risk of distortion and can help ensure the accuracy of data.

Disseminating Data

- Conduct regular reviews of privacy and security protocols and assessments before disseminating any data. Even if informed consent was obtained, circumstances may have changed that could cause an individual to rescind that consent.

> *"Video distribution in and of itself can also contribute to creating further layers of victimization: the individuals in the torture videos shot by authorities are already being doubly humiliated – in the first instance by what happens to them in custody, and in the second, by the act of filming. They are then further exposed as the footage achieves widespread circulation."* (Gregory, 28)

- Evaluate the potential for direct or indirect re-victimization and secondary harm, such as by disseminating very graphic materials (photos, videos etc.). Conduct a strategic analysis about how the release of data may accidentally be misused by others for propaganda, inciting violence or hatred, etc. This can cause a loss of dignity, privacy and agency to users, affected communities and others as well as contribute to community violence.
- Be sure to consider the privacy and security of any individual appearing in a video or photo before disseminating it. Innocent bystanders or witnesses are also vulnerable to harm if the image is released.
- Be explicit about the level of reliability and accuracy of information used or shared. Otherwise you risk presenting a false or incomplete image of the issues you intend to address.
- Ensure that organizations or entities with whom you share data have adequate privacy and security protocols in place to handle the data and mitigate risks of data transfer.
- Follow ethical practices for any market research that is done via your platform.
- Do not monetize users' data without their knowledge, consent and direct benefit.

Provide Options for Support and Legal Recourse

- Be proactive about being accountable to users and affected communities.
- Establish a mechanism to receive suggestions and complaints to improve your methodology and tools.
- If it becomes apparent that an individual is actively being exploited or is in immediate danger, you must decide whether to identify the individual. Understand and articulate your commitment to them if they are at risk or harmed. Balance whether the opportunity to provide assistance and the degree of danger is outweighed by the risks of invading the person's privacy or exposing them to further harm.
- Understand the legal recourses available to users and how they can protect their rights. For example, IDPs or refugees often have no state or little state infrastructure to protect their rights.

Archiving

Archiving is an on-going process for ensuring the secure long-term preservation, use and accessibility of the data you collect.

- Plan for archiving or data destruction early in the process, including what, where and how you want to archive your data. Don't wait until the end of the program, when time and resources may be limited.

- Consider whether you want to archive your data or destroy it. Destroying data can be more secure. However, archiving can be beneficial if the data has on-going evidentiary, historical or cultural value. It can contribute to future efforts to redress rights abuses, protect rights or support reconciliation.

- Store and archive data in formats that are future-proof (such as those used by popular software or which are unlikely to change) so that over the years you can still access and use the data.

- Videos, photos and other types of digital files can be quite large, so make sure that you have planned for sufficient space to store them.

- Make sure that you have budgeted and planned for ongoing support for your archive, whether in-house or external. This means considering ongoing and future costs, time and skills to maintain the archive.

Resources & Sources

General

Amnesty International, Benetech and The Engine Room, DATNAV: Guide to Navigating Digital Data in Human Rights Research (2016), https://library.witness.org/product/datnav-guide-to-navigating-digital-data-in-human-rights-research/

Sam Gregory, Cameras Everywhere: Ubiquitous Video Documentation of Human Rights, New Forms of Video Advocacy, and Considerations of Safety, Security, Dignity and Consent, Journal of Human Rights Practice (2010), http://jhrp.oxfordjournals.org/content/2/2/191.abstract

ICRC, Professional Standards for Protection Work, 2nd Ed (2013), https://www.icrc.org/en/publication/0999-professional-standards-protection-work-carried-out-humanitarian-and-human-rights

Mark Latonero & Zachary Gold, Data, Human Rights and Human Security (2015), https://encryptallthethings.net/docs/EATT.pdf

Oxfam's Responsible Program Data Policy (2014), https://www.oxfam.org/sites/www.oxfam.org/files/file_attachments/story/oxfam-responsible-program-data-policy-feb-2015-en_1.pdf

Principles for Digital Development, http://digitalprinciples.org

Responsible Data Forum: Hand-book Of the Modern Development Specialist Being, a Complete, Illustrated Guide to Responsible Data Usage, Manners, and General Deportment, https://responsibledata.io/resources/handbook/

UN Economic and Social Council, Revised Version of the Guidelines for the Regulation of Computerized Personal Data Files, E/CN.4/1990/72 (1990), https://documents-dds-ny.un.org/doc/UNDOC/GEN/G90/107/08/PDF/G9010708.pdf?OpenElement

UN General Assembly, Guidelines for the Regulation of Computerized Personal Data Files adopted by General Assembly resolution 45/95 on 15 December 1989, http://www.un.org/documents/ga/res/45/a45r095.htm

Adele Waugaman, Implementing the Digital Development Principles (2016), http://digitalprinciples.org/wp-content/uploads/2016/02/mSTAR-Principles_Report-v6.pdf

WITNESS, Video as Evidence: Ethical Guidelines, https://library.witness.org/product/video-as-evidence-ethical-guidelines/

WITNESS, Video as Evidence: Ethical Guidelines Checklist, https://library.witness.org/product/video-as-evidence-ethical-guidelines-checklist/

Conflict Sensitivity Analysis

Conflict Sensitivity Consortium, Checklist for Selecting a Conflict Analysis Tool (2015), http://local.conflictsensitivity.org/other_publication/checklist-for-selecting-a-conflict-analysis-tool/

International Alert, Conflict-Sensitive Business Practice: Guidance for Extractive Industries (2005) (Private sector oriented, but still useful for NGO and public sector), http://www.international-alert.org/resources/publications/csbp-extractive-industries-en

Peacebuilding Center, Peace and Conflict Impact Assessment (PCIA) Handbook, Version 4 (2013), http://reliefweb.int/report/world/peace-and-conflict-impact-assessment-pcia-handbook-version-4-2013

SIDA Manual for Conflict Analysis (2006), http://local.conflictsensitivity.org/wp-content/uploads/2015/05/Manual_for_Conflict_Analysis.pdf

Informed Consent

Urban Reproductive Health Initiative's Responsible Data Forum: Framework for Consent Policies, https://wiki.responsibledata.io/Framework_for_consent_policies

WITNESS, Obtaining Informed Consent, https://library.witness.org/product/obtaining-informed-consent/

Privacy

GSMA Foundation Mobile and Privacy: Privacy Design Guidelines for Mobile Application Development (2012), http://gsma.com/mobileprivacy

International Organization for Standardization, ISO/IEC 29100:2011, Information technology—Security techniques—Privacy framework, http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=45123

Madrid Resolution: International Standards on the Protection of Personal Data and Privacy (2009), http://privacyconference2011.org/htmls/adoptedResolutions/2009_Madrid/2009_M1.pdf

OHCHR, The right to privacy in the digital age (2014), https://s3.amazonaws.com/access.3cdn.net/bodc79954929ed5019_90m6byjs4.pdf

Oxford Internet Institute: Ethical Privacy Guidelines for Mobile Connectivity Measurements (2013), https://www.oii.ox.ac.uk/archive/downloads/research/files/Ethical_Privacy_Guidelines_for_Mobile_Connectivity_Measurements.pdf

White House Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy. Consumer Privacy Bill of Rights, pg. 9 (2012), http://www.whitehouse.gov/sites/default/files/privacy-final.pdf

Privacy Information Assessments

Electronic Cash Transfer Learning Action Network, Tip Sheet: Privacy Impact Assessment (2016), http://elan.cashlearning.org/wp-content/uploads/2016/05/Privacy-impact-tipsheet.pdf

New Zealand Privacy Commissioner, Privacy Impact Assessment Toolkit (2015), https://www.privacy.org.nz/assets/Files/Guidance/Privacy-Impact-Part-1.pdf

UNHCR Privacy Impact Assessment of UNHCR Cash Based Interventions, http://www.globalprotectioncluster.org/_assets/files/tools_and_guidance/cash-based-interventions/erc-privacy-impact-assessment-of-unhcr-cbi_en.pdf

US DHS, Privacy Impact Assessments, The Privacy Office Official Guidance (2010), https://www.dhs.gov/sites/default/files/publications/privacy_pia_guidance_june2010_0.pdf

US DHS, Privacy Impact Assessment Template, https://www.dhs.gov/sites/default/files/publications/privacy_pia_template_0.pdf

UK ICO, Conducting Privacy Impact Assessments Code of Practice (2014), https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

Security & Data Protection

Electronic Frontier Foundation, An Introduction to Threat Modeling, https://ssd.eff.org/en/module/introduction-threat-modeling

Electronic Frontier Foundation, Secure App Scorecard, https://www.eff.org/secure-messaging-scorecard

Electronic Frontier Foundation, Surveillance Self-Defense Guide, https://ssd.eff.org/

Electronic Frontier Foundation, Who Has Your Back? 2015: Protecting Your Data from [US] Government Requests, https://www.eff.org/wp/

who-has-your-back-2015-protecting-your-data-government-requests

Encrypt All the Things, Data Security Action Plan, *https://encryptallthethings.net/docs/EATT.pdf*

ESOMAR Data Protection Checklist, *https://www.esomar.org/uploads/public/knowledge-and-standards/codes- and-guidelines/ESOMAR-Data-Protection-Checklist_January-2015.pdf*

InterAction's Protection Working Group, *http://pqdl.care.org/Practice/Data Collection in Humanitarian Response, A Guide for Incorporating Protection.pdf*

International Organization for Standardization, ISO/IEC 27001:2013, Information technology—Security techniques—Information security management systems—Requirements, *http://www.iso.org/iso/catalogue_detail?csnumber=54534*

International Organization for Standardization, ISO/IEC 27005:2011, Information technology—Security techniques—Information security risk management, *http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=56742*

International Organization for Standardization, ISO/IEC 27018:2014, Information technology—Security techniques—Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors, *http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=61498*

Security-in-a-box Security Tactics, https://securityinabox.org/en/tactics

Destroy Sensitive Information, *https://securityinabox.org/en/guide/destroy-sensitive-information*

Protect the Sensitive Files on your Computer, *https://securityinabox.org/en/guide/secure-file-storage*

Recover from Information Loss, *https://securityinabox.org/en/guide/backup*

Tactical Tech, Holistic Security Manual, *https://holistic-security.tacticaltech.org*

WITNESS, Transferring Human Rights Video Online, *https://library.witness.org/product/transferring-human-rights-video-online/*

WITNESS, Video as Evidence: Transferring Files, *https://library.witness.org/product/video-as-evidence-tech-tools-transferring-files/*

Data Collection

ESOMAR Passive data collection, observation and recording, *https://www.esomar.org/uploads/public/knowledge-and-standards/codes-and-guidelines/ESOMAR_Codes-and-Guidelines_Maintaining-Distinctions-MRDM.pdf*

ESOMAR Interviewing children and young people, *https://www.esomar.org/uploads/public/knowledge-and-standards/codes-and-guidelines/ESOMAR_Codes-and-Guidelines_Interviewing-Children-and-Young-People.pdf*

ESOMAR Guide on distinguishing market research from other data collection activities, *https://www.esomar.org/ uploads/public/knowledge-and-standards/codes-and-guidelines/ESOMAR_Codes-and-Guidelines_Maintaining- Distinctions-MRDM.pdf*

Urban Reproductive Health, Third Party Data Request Form, *https://www.urbanreproductivehealth.org/sites/mle/files/third_party_data_request_form_-_senegal_july_2015.pdf*

Archiving

Responsible Data Forum: Hand-book Of the Modern Development Specialist Being, a Complete, Illustrated Guide to Responsible Data Usage, Manners, and General Deportment; Closing a Project, *https://responsibledata.io/resources/handbook/chapters/chapter-03-closing-a-project.html*