Additional Content for Responsible Development Data – Practitioner’s Guide

# How to group this section? ~~Data Analysis~~

## Digital Risk Assessment and Safety Planning

Practical considerations, questions, tools and tactics described here can help humanitarian and development practitioners assess and prioritize probable risks and direct threats, as well as develop structured steps and behaviors to help keep themselves and participants safe while engaging in project activities. Holistic security specialists can work together with staff, consultants, project participants, partners, and other stakeholders in the design, development, implementation, monitoring and evaluation stages of any project using ICTs, or collecting digital information from participants, can use these as guidance for identifying risk profiles of staff, consultants, partners’ and participants’, and reducing risk to an acceptable level for each individual or group.

## Project participant-centered privacy and security

A 2013 report emphasizes the important of designing privacy and security protocols and training starting from the perspectives and experiences of end-users (staff, consultants, project participants, partners) themselves . This implies working together with humanitarian or development project ICTs end-users of to develop an in-depth understanding of their unique data protection and risk management needs, including their digital behaviors, risk profiles, and safety planning. This includes gleaning an understanding of end-users’ definitions (or lack of definitions) of digital technologies and what they perceive to be risky or unsafe behaviors. It is critical to tailor education, training and mentorship around holistic security (digital; operational-physical; psychosocial) and privacy to end-users’ contexts and demographics, for example, by sex, age, ethnicity, political affiliation, urban versus rural, wealthy versus poor, previous exposure to the Internet versus no experience, and other locally relevant subcategories. Community mentors, champions and allies should be identified and engaged in the process so that they can provide support when external holistic security specialists are not present. Holistic safety messages can raise the usefulness of the Internet and mobile for areas such as commerce, education, jobs, and a resource for denouncing online or offline abuse while raising awareness of how to assess and mitigate risks related to using digital tools and spaces. Holistic security campaigns should be widely run on media channels such as radio, print and television as well as online. End-user privacy and safety champions should be supported as leaders of and spokespeople for these campaigns.

## Privacy by Design

“Privacy by Design” (PbD) is a framework that was developed in the 1990s to address the growing effects of information and communication technologies and large-scale networked data systems. It advances the view that the future of privacy cannot be assured simply through compliance with regulatory frameworks. Instead, it must become an organization’s default mode of operation. PbD aims to help protect user privacy and at the same time, maximize utility if any data collected for research. Privacy by Design implies a multi-dimensional consideration of how all the elements of platform design operate together. It requires protection of personal information from the start and analysis at every step of the design process. In addition, the process guides designers to look at how all aspects of the design impact all other aspects and to assess the effect of any change to the platform on all the other aspects of the platform as part of an iterative process .

PbD works through three core aspects: IT systems, accountable business practices, and physical design and networked infrastructure and seven “foundational principles” (see side box).

Organizations such as the GSMA have used PbD principles to create guidelines for mobile application development (See Annex 1). A similar process could be used for GEM during design and development to ensure that privacy protocols are integrated right from the design stage and then tested on the ground during the first stage of piloting and iteration.

Though the GEM platform should follow PbD concepts and bake privacy into its design, some of the core concepts that relate to consent and data may be confusing or difficult to imagine in contexts where there is low literacy and little prior experience with the Internet or social networking. It will be critical to work with girls and their communities to ensure people understand these concepts and their implications.

## Threat Analysis and Risk Mitigation

Some organizations conduct “threat” analyses to identify who the possible actors or “adversaries” are that may wish to access a particular dataset for a harmful purpose. The threat analysis allows the organization to then analyze the levels of security that should be put into place in order to protect against adversaries and threats. The Electronic Frontier Foundation “surveillance self-defense” toolkit offers guidance on how to analyze assets, threats, risks and adversaries and design ways to protect against them. The toolkit also offers a number of tips on keeping data and information private, such as using encryption and circumvention tools, hidden browsing, secure data and file deletion, and secure use of mobile devices. Although risk of end-users being targeted for government surveillance may seem small in some contexts, it has been shown that populations in all but four countries globally are subjected to electronic surveillance. Circumventing surveillance and creating spaces for digital privacy will be useful to consider for design of end-user platform to ensure a higher level of security and lower risk to users. In addition, engaging end-user communities and their allies in good privacy-protecting attitudes and behaviors will be key in helping end-users protect themselves while using online platforms, other social media or mobile technologies. Concepts or good practices used by human rights workers and journalists working in risky environments are adaptable to humanitarian and development project convests in terms of platform design, network security, privacy by design, and end-user centric, responsible data practices.

## Storage

**Personal Cloud** — Set up a local shared server to sync data/files to (e.g. PirateBox). write more on this later

*Checksum Verification*— A way to ensure that the files you download have not been tampered with. The uploader will create a checksum hash (typically MD5 or SHA1) that is transmitted through secure means to the downloader. The downloader then pulls the checksum hash from the downloaded file to verify that they are the same and untampered with.

*File Sharing* – secure file sharing versus communicating finished reports (resource for secure file sharing, OnionShare run over Tor for file encryption and sharing)